Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/JP05/001041

International filing date: 20 January 2005 (20.01.2005)

Document type: Certified copy of priority document

Document details: Country/Office: JP
Number: 2004-045974
Filing date: 23 February 2004 (23.02.2004)

Date of receipt at the International Bureau: 10 March 2005 (10.03.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

PCT/JP2005/001041

日　本　国　特　許　庁
JAPAN PATENT OFFICE

20.01.2005

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出　願　年　月　日
Date of Application:　２００４年　２月２３日

出　願　番　号
Application Number:　特願２００４－０４５９７４

[ST. 10/C]:　［Ｊ Ｐ ２００４－０４５９７４］

出　願　人
Applicant(s):　大日本印刷株式会社

２００５年　２月２５日

特許庁長官
Commissioner,
Japan Patent Office　小川　洋

出証番号　出証特２００５－３０１５１３６

【書類名】　特許願
【整理番号】　A16008
【あて先】　特許庁長官殿
【国際特許分類】　G06F 15/00
【発明者】
　【住所又は居所】　東京都新宿区市谷加賀町一丁目１番１号　大日本印刷株式会社内
　【氏名】　庭田　尚蔵
【発明者】
　【住所又は居所】　東京都新宿区市谷加賀町一丁目１番１号　大日本印刷株式会社内
　【氏名】　矢野　義博
【発明者】
　【住所又は居所】　東京都新宿区市谷加賀町一丁目１番１号　大日本印刷株式会社内
　【氏名】　近田　恭之
【発明者】
　【住所又は居所】　東京都新宿区市谷加賀町一丁目１番１号　大日本印刷株式会社内
　【氏名】　半田　富己男
【発明者】
　【住所又は居所】　東京都新宿区市谷加賀町一丁目１番１号　大日本印刷株式会社内
　【氏名】　吉川　和寿
【特許出願人】
　【識別番号】　000002897
　【氏名又は名称】　大日本印刷株式会社
【代理人】
　【識別番号】　100091476
　【弁理士】
　【氏名又は名称】　志村　浩
【手数料の表示】
　【予納台帳番号】　062776
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　特許請求の範囲　1
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1

【書類名】特許請求の範囲
【請求項１】
ネットワーク網と、このネットワーク網に接続されたサーバコンピュータと、このネットワーク網に接続可能な複数のクライアントコンピュータと、このクライアントコンピュータに接続して用いるために個々のユーザに発行された携帯可能情報記録媒体と、を備えるコンピュータシステムであって、
前記各クライアントコンピュータには、それぞれ他のクライアントコンピュータと識別可能な固有の識別コードが記録されており、
前記各携帯可能情報記録媒体には、それぞれ特定のクライアントコンピュータに記録されている特定の識別コードに対応する識別コードが記録されており、
前記各クライアントコンピュータには、携帯可能情報記録媒体を接続するためのインターフェイス手段と、現在接続中の携帯可能情報記録媒体に記録されている識別コードと自分自身に記録されている識別コードとを照合する識別コード照合手段と、この照合結果に基づいて所定のアクセス権を設定するアクセス権設定手段と、設定されたアクセス権の範囲内で前記サーバコンピュータに対するアクセスを行うサーバアクセス手段と、が備わっていることを特徴とするコンピュータシステム。
【請求項２】
ネットワーク網と、このネットワーク網に接続されたサーバコンピュータと、このネットワーク網に接続可能な複数のクライアントコンピュータと、このクライアントコンピュータに接続して用いるために個々のユーザに発行された携帯可能情報処理装置と、を備えるコンピュータシステムであって、
前記各クライアントコンピュータには、それぞれ他のクライアントコンピュータと識別可能な固有の識別コードが記録されており、
前記各携帯可能情報処理装置には、それぞれ特定のクライアントコンピュータに記録されている特定の識別コードに対応する識別コードが記録されており、
前記各クライアントコンピュータには、携帯可能情報処理装置を接続するためのインターフェイス手段と、現在接続中の携帯可能情報処理装置から伝達されてきたアクセス権の範囲内で前記サーバコンピュータに対するアクセスを行うサーバアクセス手段と、が備わっており、
前記携帯可能情報処理装置には、現在接続中のクライアントコンピュータに記録されている識別コードと自分自身に記録されている識別コードとを照合する識別コード照合手段と、この照合結果に基づいて所定のアクセス権を設定するアクセス権設定手段と、設定されたアクセス権を現在接続中のクライアントコンピュータに伝達するアクセス権伝達手段と、が備わっていることを特徴とするコンピュータシステム。
【請求項３】
請求項１または２に記載のコンピュータシステムにおいて、
アクセス権設定手段が、照合結果が一致した場合には第１のアクセス権を設定し、照合結果が一致しなかった場合には前記第１のアクセス権よりも制限事項の多い第２のアクセス権を設定することを特徴とするコンピュータシステム。
【請求項４】
請求項１～３のいずれかに記載のコンピュータシステムにおいて、
クライアントコンピュータに内蔵されているＬＡＮ通信回路に付与されたＭＡＣアドレス、クライアントコンピュータの記憶装置に格納されている固有のデータ、もしくは、クライアントコンピュータの記憶装置に格納されているアプリケーションプログラムの構成を示す情報を、当該クライアントコンピュータを識別するための固有の識別コードとして用いることを特徴とするコンピュータシステム。
【請求項５】
ネットワーク網と、このネットワーク網に接続されたサーバコンピュータと、このネットワーク網に接続可能な複数のクライアントコンピュータと、このクライアントコンピュータに接続して用いるために個々のユーザに発行された携帯可能情報記録媒体と、を備え

るコンピュータシステムであって、
　前記各携帯可能情報記録媒体には、それぞれクライアントコンピュータを前記ネットワーク網の特定箇所に接続した場合に得られる特定のネットワーク環境を示す環境情報が記録されており、
　前記各クライアントコンピュータには、携帯可能情報記録媒体を接続するためのインターフェイス手段と、現在接続中の携帯可能情報記録媒体に記録されている環境情報によって示されるネットワーク環境と自分自身の現在のネットワーク環境とを照合する環境照合手段と、この照合結果に基づいて所定のアクセス権を設定するアクセス権設定手段と、設定されたアクセス権の範囲内で前記サーバコンピュータに対するアクセスを行うサーバアクセス手段と、が備わっていることを特徴とするコンピュータシステム。
【請求項６】
　ネットワーク網と、このネットワーク網に接続されたサーバコンピュータと、このネットワーク網に接続可能な複数のクライアントコンピュータと、このクライアントコンピュータに接続して用いるために個々のユーザに発行された携帯可能情報処理装置と、を備えるコンピュータシステムであって、
　前記各携帯可能情報処理装置には、それぞれクライアントコンピュータを前記ネットワーク網の特定箇所に接続した場合に得られる特定のネットワーク環境を示す環境情報が記録されており、
　前記各クライアントコンピュータには、携帯可能情報処理装置を接続するためのインターフェイス手段と、現在接続中の携帯可能情報処理装置から伝達されてきたアクセス権の範囲内で前記サーバコンピュータに対するアクセスを行うサーバアクセス手段と、が備わっており、
　前記携帯可能情報処理装置には、現在接続中のクライアントコンピュータのネットワーク環境と自分自身に記録されている環境情報によって示されるネットワーク環境とを照合する環境照合手段と、この照合結果に基づいて所定のアクセス権を設定するアクセス権設定手段と、設定されたアクセス権を現在接続中のクライアントコンピュータに伝達するアクセス権伝達手段と、が備わっていることを特徴とするコンピュータシステム。
【請求項７】
　請求項５または６に記載のコンピュータシステムにおいて、
　アクセス権設定手段が、照合結果が一致した場合には第１のアクセス権を設定し、照合結果が一致しなかった場合には前記第１のアクセス権よりも制限事項の多い第２のアクセス権を設定することを特徴とするコンピュータシステム。
【請求項８】
　請求項５～７のいずれかに記載のコンピュータシステムにおいて、
　クライアントコンピュータに付与されたＩＰアドレス、クライアントコンピュータに設定されたデフォルトゲートウエイアドレス、クライアントコンピュータに設定されたプロキシサーバアドレス、もしくは、クライアントコンピュータが利用するＤＮＳサーバによって照会可能なドメイン名を、当該クライアントコンピュータのネットワーク環境を示す環境情報として用いることを特徴とするコンピュータシステム。
【請求項９】
　ネットワーク網と、このネットワーク網に接続されたサーバコンピュータと、このネットワーク網に接続可能な複数のクライアントコンピュータと、このクライアントコンピュータに接続して用いるために個々のユーザに発行された携帯可能情報記録媒体と、を備えるコンピュータシステムであって、
　前記各クライアントコンピュータには、それぞれ他のクライアントコンピュータと識別可能な固有の識別コードが記録されており、
　前記各携帯可能情報記録媒体には、それぞれ特定のクライアントコンピュータに記録されている特定の識別コードに対応する識別コードと、それぞれクライアントコンピュータを前記ネットワーク網の特定箇所に接続した場合に得られる特定のネットワーク環境を示す環境情報と、が記録されており、

前記各クライアントコンピュータには、携帯可能情報記録媒体を接続するためのインターフェイス手段と、現在接続中の携帯可能情報記録媒体に記録されている識別コードと自分自身に記録されている識別コードとを照合する識別コード照合手段と、現在接続中の携帯可能情報記録媒体に記録されている環境情報によって示されるネットワーク環境と自分自身の現在のネットワーク環境とを照合する環境照合手段と、これらの照合結果に基づいて所定のアクセス権を設定するアクセス権設定手段と、設定されたアクセス権の範囲内で前記サーバコンピュータに対するアクセスを行うサーバアクセス手段と、が備わっていることを特徴とするコンピュータシステム。

【請求項１０】

ネットワーク網と、このネットワーク網に接続されたサーバコンピュータと、このネットワーク網に接続可能な複数のクライアントコンピュータと、このクライアントコンピュータに接続して用いるために個々のユーザに発行された携帯可能情報処理装置と、を備えるコンピュータシステムであって、

前記各クライアントコンピュータには、それぞれ他のクライアントコンピュータと識別可能な固有の識別コードが記録されており、

前記各携帯可能情報処理装置には、それぞれ特定のクライアントコンピュータに記録されている特定の識別コードに対応する識別コードと、それぞれクライアントコンピュータを前記ネットワーク網の特定箇所に接続した場合に得られる特定のネットワーク環境を示す環境情報と、が記録されており、

前記各クライアントコンピュータには、携帯可能情報処理装置を接続するためのインターフェイス手段と、現在接続中の携帯可能情報処理装置から伝達されてきたアクセス権の範囲内で前記サーバコンピュータに対するアクセスを行うサーバアクセス手段と、が備わっており、

前記携帯可能情報処理装置には、現在接続中のクライアントコンピュータに記録されている識別コードと自分自身に記録されている識別コードとを照合する識別コード照合手段と、現在接続中のクライアントコンピュータのネットワーク環境と自分自身に記録されている環境情報によって示されるネットワーク環境とを照合する環境照合手段と、これらの照合結果に基づいて所定のアクセス権を設定するアクセス権設定手段と、設定されたアクセス権を現在接続中のクライアントコンピュータに伝達するアクセス権伝達手段と、が備わっていることを特徴とするコンピュータシステム。

【請求項１１】

請求項９または１０に記載のコンピュータシステムにおいて、

アクセス権設定手段が、識別コード照合手段による照合結果が一致した場合には第１のアクセス権を設定し、識別コード照合手段による照合結果は一致しないが環境照合手段による照合結果が一致した場合には前記第１のアクセス権よりも制限事項の多い第２のアクセス権を設定し、いずれの照合結果も一致しなかった場合には前記第２のアクセス権よりも更に制限事項の多い第３のアクセス権を設定することを特徴とするコンピュータシステム。

【請求項１２】

請求項９または１０に記載のコンピュータシステムにおいて、

アクセス権設定手段が、識別コード照合手段による照合結果と環境照合手段による照合結果との双方が一致した場合には第１のアクセス権を設定し、識別コード照合手段による照合結果は一致したが環境照合手段による照合結果は一致しない場合には前記第１のアクセス権よりも制限事項の多い第２のアクセス権を設定し、いずれの照合結果も一致しなかった場合には前記第２のアクセス権よりも更に制限事項の多い第３のアクセス権を設定することを特徴とするコンピュータシステム。

【請求項１３】

ネットワーク網と、このネットワーク網に接続されたサーバコンピュータと、このネットワーク網に接続可能な複数のクライアントコンピュータと、を備えるコンピュータシステムについて、個々のユーザがクライアントコンピュータを利用してサーバコンピュータ

へアクセスする際のアクセス権を設定する方法であって、
　個々のユーザに対して、クライアントコンピュータに接続して用いるための携帯可能情報処理装置を発行し、この携帯可能情報処理装置に、特定のクライアントコンピュータに記録されている識別コードであって当該特定のクライアントコンピュータを他のクライアントコンピュータと識別することが可能な固有の識別コードに対応する識別コードを記録しておく準備段階と、
　ユーザが、自分に対して発行された所定の携帯可能情報処理装置を所定のクライアントコンピュータに接続し、前記所定のクライアントコンピュータに対する利用開始手続を行ったときに、前記所定のクライアントコンピュータもしくは前記所定の携帯可能情報処理装置によって、前記所定のクライアントコンピュータに記録されている識別コードと前記所定の携帯可能情報処理装置に記録されている識別コードとを照合させ、この照合結果に基づいて所定のアクセス権を設定させるアクセス権設定段階と、
　を有し、前記アクセス権設定段階において、照合結果が一致しなかった場合には、照合結果が一致した場合に比べて、制限事項の多いアクセス権の設定を行うようにすることを特徴とするコンピュータシステムにおけるアクセス権設定方法。

【請求項１４】
　ネットワーク網と、このネットワーク網に接続されたサーバコンピュータと、このネットワーク網に接続可能な複数のクライアントコンピュータと、を備えるコンピュータシステムについて、個々のユーザがクライアントコンピュータを利用してサーバコンピュータへアクセスする際のアクセス権を設定する方法であって、
　個々のユーザに対して、クライアントコンピュータに接続して用いるための携帯可能情報処理装置を発行し、この携帯可能情報処理装置に、クライアントコンピュータを前記ネットワーク網の特定箇所に接続した場合に得られる特定のネットワーク環境を示す環境情報を記録しておく準備段階と、
　ユーザが、自分に対して発行された所定の携帯可能情報処理装置を所定のクライアントコンピュータに接続し、前記所定のクライアントコンピュータに対する利用開始手続を行ったときに、前記所定のクライアントコンピュータもしくは前記所定の携帯可能情報処理装置によって、前記所定のクライアントコンピュータの現在のネットワーク環境と前記所定の携帯可能情報処理装置に記録されている環境情報によって示されるネットワーク環境とを照合させ、この照合結果に基づいて所定のアクセス権を設定させるアクセス権設定段階と、
　を有し、前記アクセス権設定段階において、照合結果が一致しなかった場合には、照合結果が一致した場合に比べて、制限事項の多いアクセス権の設定を行うようにすることを特徴とするコンピュータシステムにおけるアクセス権設定方法。

【請求項１５】
　ネットワーク網と、このネットワーク網に接続されたサーバコンピュータと、このネットワーク網に接続可能な複数のクライアントコンピュータと、を備えるコンピュータシステムについて、個々のユーザがクライアントコンピュータを利用してサーバコンピュータへアクセスする際のアクセス権を設定する方法であって、
　個々のユーザに対して、クライアントコンピュータに接続して用いるための携帯可能情報処理装置を発行し、この携帯可能情報処理装置に、特定のクライアントコンピュータに記録されている識別コードであって当該特定のクライアントコンピュータを他のクライアントコンピュータと識別することが可能な固有の識別コードに対応する識別コードと、クライアントコンピュータを前記ネットワーク網の特定箇所に接続した場合に得られる特定のネットワーク環境を示す環境情報と、を記録しておく準備段階と、
　ユーザが、自分に対して発行された所定の携帯可能情報処理装置を所定のクライアントコンピュータに接続し、前記所定のクライアントコンピュータに対する利用開始手続を行ったときに、前記所定のクライアントコンピュータもしくは前記所定の携帯可能情報処理装置によって、前記所定のクライアントコンピュータに記録されている識別コードと前記所定の携帯可能情報処理装置に記録されている識別コードとを照合させるとともに、前記

所定のクライアントコンピュータの現在のネットワーク環境と前記所定の携帯可能情報処理装置に記録されている環境情報によって示されるネットワーク環境とを照合させ、これらの照合結果に基づいて所定のアクセス権を設定させるアクセス権設定段階と、

を有し、前記アクセス権設定段階において、識別コードの照合結果が一致した場合には第１のアクセス権を設定し、識別コードの照合結果は一致しないがネットワーク環境の照合結果が一致した場合には前記第１のアクセス権よりも制限事項の多い第２のアクセス権を設定し、いずれの照合結果も一致しなかった場合には前記第２のアクセス権よりも更に制限事項の多い第３のアクセス権を設定することを特徴とするコンピュータシステムにおけるアクセス権設定方法。

【請求項１６】

ネットワーク網と、このネットワーク網に接続されたサーバコンピュータと、このネットワーク網に接続可能な複数のクライアントコンピュータと、を備えるコンピュータシステムについて、個々のユーザがクライアントコンピュータを利用してサーバコンピュータへアクセスする際のアクセス権を設定する方法であって、

個々のユーザに対して、クライアントコンピュータに接続して用いるための携帯可能情報処理装置を発行し、この携帯可能情報処理装置に、特定のクライアントコンピュータに記録されている識別コードであって当該特定のクライアントコンピュータを他のクライアントコンピュータと識別することが可能な固有の識別コードに対応する識別コードと、クライアントコンピュータを前記ネットワーク網の特定箇所に接続した場合に得られる特定のネットワーク環境を示す環境情報と、を記録しておく準備段階と、

ユーザが、自分に対して発行された所定の携帯可能情報処理装置を所定のクライアントコンピュータに接続し、前記所定のクライアントコンピュータに対する利用開始手続を行ったときに、前記所定のクライアントコンピュータもしくは前記所定の携帯可能情報処理装置によって、前記所定のクライアントコンピュータに記録されている識別コードと前記所定の携帯可能情報処理装置に記録されている識別コードとを照合させるとともに、前記所定のクライアントコンピュータの現在のネットワーク環境と前記所定の携帯可能情報処理装置に記録されている環境情報によって示されるネットワーク環境とを照合させ、これらの照合結果に基づいて所定のアクセス権を設定させるアクセス権設定段階と、

を有し、前記アクセス権設定段階において、識別コード照合手段による照合結果と環境照合手段による照合結果との双方が一致した場合には第１のアクセス権を設定し、識別コード照合手段による照合結果は一致したが環境照合手段による照合結果は一致しない場合には前記第１のアクセス権よりも制限事項の多い第２のアクセス権を設定し、いずれの照合結果も一致しなかった場合には前記第２のアクセス権よりも更に制限事項の多い第３のアクセス権を設定することを特徴とするコンピュータシステムにおけるアクセス権設定方法。

【請求項１７】

請求項１～１２のいずれかに記載のコンピュータシステムにおけるクライアントコンピュータとしてコンピュータを機能させるためのプログラムまたは当該プログラムを記録したコンピュータ読み取り可能な記録媒体。

【書類名】明細書
【発明の名称】コンピュータシステムおよびそのアクセス権設定方法
【技術分野】
【０００１】
本発明は、コンピュータシステムおよびそのアクセス権設定方法に関し、特に、クライアントコンピュータからネットワークを介してサーバコンピュータにアクセスする際のセキュリティを確保する技術に関する。
【背景技術】
【０００２】
現在、コンピュータは、ネットワークを用いて相互に接続して利用するのが一般的であり、企業のみならず、一般家庭においても、ハブ、ＬＡＮスイッチ、ルータなどを組み込んだネットワーク網の構築が行われるようになってきている。通常、企業では、社内ＬＡＮやＷＡＮといった専用のネットワーク網を構築し、このネットワーク網に、各事業部の業務形態に合わせて、種々の機能をもったサーバコンピュータを接続して用いるのが一般的である。個々の社員は、このネットワーク網にパソコンなどのクライアントコンピュータを接続し、サーバコンピュータとデータのやりとりを行いながら業務を遂行することになる。
【０００３】
このようなネットワーク網を利用したコンピュータシステムを運用する上では、セキュリティの管理が非常に重要である。すなわち、ネットワーク網に接続された各コンピュータを、外部のハッカーによる不正アクセスから防御することはもちろんのこと、同一企業に所属する社員であっても、その所属や職責に応じて、それぞれ固有のアクセス制限を課するような運用が不可欠になる。
【０００４】
そこで、ネットワーク網を利用したコンピュータシステムにおけるセキュリティ管理の技術が種々提案されている。たとえば、下記の特許文献１および２には、クライアントコンピュータとサーバコンピュータとがネットワーク接続されているコンピュータシステムにおいて、個々のユーザごとにそれぞれ固有のアクセス権の管理を行うための技術が開示されている。
【特許文献１】特開２０００－１０９３０号公報
【特許文献２】特開２００３－１２２６３５号公報
【発明の開示】
【発明が解決しようとする課題】
【０００５】
前掲の特許公報に開示されている技術をはじめ、従来のセキュリティ管理の手法は、いずれも個々のユーザごとに所定のアクセス権を設定する、という基本的な考え方に基づいている。すなわち、各ユーザにそれぞれ所定のアカウント（ユーザ名）とパスワードを付与し、個々のアカウントについてそれぞれ所定のアクセス権の設定を行っておき、特定のアカウントによるログイン手続があった場合には、パスワードの照合によりこのログイン手続が正規のものであることを確認した後、当該アカウントに設定されているアクセス権の範囲内でアクセスを許可する、という運用を行うのが一般的である。
【０００６】
このように個々のユーザごとに特定のアクセス権を設定する、という基本方針は、大局的な見地からは、非常に合理的な手法であるが、コンピュータシステムを利用した業務形態の内容が益々複雑化する昨今では、必ずしもこのような基本方針だけでは対応しきれないことも少なくない。特に、多数の社員をかかえる企業では、不正な行為を行う社員の存在を完全には否定することができないので、個々の社員を完全に信頼して、どのような状況下においても無条件に同一のアクセス権を与えてしまうことは危険である。
【０００７】
そこで本発明は、個々のユーザに対して、状況に応じて（利用するコンピュータやネッ

トワーク環境に応じて）、異なるアクセス権を設定することが可能なコンピュータシステムを提供することを目的とする。
【課題を解決するための手段】
【０００８】
(1)　本発明の第１の態様は、ネットワーク網と、このネットワーク網に接続されたサーバコンピュータと、このネットワーク網に接続可能な複数のクライアントコンピュータと、このクライアントコンピュータに接続して用いるために個々のユーザに発行された携帯可能情報記録媒体と、を備えるコンピュータシステムにおいて、
各クライアントコンピュータに、それぞれ他のクライアントコンピュータと識別可能な固有の識別コードを記録しておき、
各携帯可能情報記録媒体に、それぞれ特定のクライアントコンピュータに記録されている特定の識別コードに対応する識別コードを記録しておき、
各クライアントコンピュータには、携帯可能情報記録媒体を接続するためのインターフェイス手段と、現在接続中の携帯可能情報記録媒体に記録されている識別コードと自分自身に記録されている識別コードとを照合する識別コード照合手段と、この照合結果に基づいて所定のアクセス権を設定するアクセス権設定手段と、設定されたアクセス権の範囲内でサーバコンピュータに対するアクセスを行うサーバアクセス手段と、を設けるようにしたものである。
【０００９】
(2)　本発明の第２の態様は、ネットワーク網と、このネットワーク網に接続されたサーバコンピュータと、このネットワーク網に接続可能な複数のクライアントコンピュータと、このクライアントコンピュータに接続して用いるために個々のユーザに発行された携帯可能情報処理装置と、を備えるコンピュータシステムにおいて、
各クライアントコンピュータに、それぞれ他のクライアントコンピュータと識別可能な固有の識別コードを記録しておき、
各携帯可能情報処理装置に、それぞれ特定のクライアントコンピュータに記録されている特定の識別コードに対応する識別コードを記録しておき、
各クライアントコンピュータには、携帯可能情報処理装置を接続するためのインターフェイス手段と、現在接続中の携帯可能情報処理装置から伝達されてきたアクセス権の範囲内でサーバコンピュータに対するアクセスを行うサーバアクセス手段と、を設け、
携帯可能情報処理装置には、現在接続中のクライアントコンピュータに記録されている識別コードと自分自身に記録されている識別コードとを照合する識別コード照合手段と、この照合結果に基づいて所定のアクセス権を設定するアクセス権設定手段と、設定されたアクセス権を現在接続中のクライアントコンピュータに伝達するアクセス権伝達手段と、を設けるようにしたものである。
【００１０】
(3)　本発明の第３の態様は、上述の第１または第２の態様に係るコンピュータシステムにおいて、
アクセス権設定手段が、照合結果が一致した場合には第１のアクセス権を設定し、照合結果が一致しなかった場合には第１のアクセス権よりも制限事項の多い第２のアクセス権を設定するようにしたものである。
【００１１】
(4)　本発明の第４の態様は、上述の第１～第３の態様に係るコンピュータシステムにおいて、
クライアントコンピュータに内蔵されているＬＡＮ通信回路に付与されたＭＡＣアドレス、クライアントコンピュータの記憶装置に格納されている固有のデータ、もしくは、クライアントコンピュータの記憶装置に格納されているアプリケーションプログラムの構成を示す情報を、当該クライアントコンピュータを識別するための固有の識別コードとして用いるようにしたものである。
【００１２】

(5)　本発明の第５の態様は、ネットワーク網と、このネットワーク網に接続されたサーバコンピュータと、このネットワーク網に接続可能な複数のクライアントコンピュータと、このクライアントコンピュータに接続して用いるために個々のユーザに発行された携帯可能情報記録媒体と、を備えるコンピュータシステムにおいて、
各携帯可能情報記録媒体に、それぞれクライアントコンピュータをネットワーク網の特定箇所に接続した場合に得られる特定のネットワーク環境を示す環境情報を記録しておき、
各クライアントコンピュータに、携帯可能情報記録媒体を接続するためのインターフェイス手段と、現在接続中の携帯可能情報記録媒体に記録されている環境情報によって示されるネットワーク環境と自分自身の現在のネットワーク環境とを照合する環境照合手段と、この照合結果に基づいて所定のアクセス権を設定するアクセス権設定手段と、設定されたアクセス権の範囲内でサーバコンピュータに対するアクセスを行うサーバアクセス手段と、を設けるようにしたものである。
【００１３】
(6)　本発明の第６の態様は、ネットワーク網と、このネットワーク網に接続されたサーバコンピュータと、このネットワーク網に接続可能な複数のクライアントコンピュータと、このクライアントコンピュータに接続して用いるために個々のユーザに発行された携帯可能情報処理装置と、を備えるコンピュータシステムにおいて、
各携帯可能情報処理装置に、それぞれクライアントコンピュータをネットワーク網の特定箇所に接続した場合に得られる特定のネットワーク環境を示す環境情報を記録しておき、
各クライアントコンピュータには、携帯可能情報処理装置を接続するためのインターフェイス手段と、現在接続中の携帯可能情報処理装置から伝達されてきたアクセス権の範囲内でサーバコンピュータに対するアクセスを行うサーバアクセス手段と、を設け、
携帯可能情報処理装置には、現在接続中のクライアントコンピュータのネットワーク環境と自分自身に記録されている環境情報によって示されるネットワーク環境とを照合する環境照合手段と、この照合結果に基づいて所定のアクセス権を設定するアクセス権設定手段と、設定されたアクセス権を現在接続中のクライアントコンピュータに伝達するアクセス権伝達手段と、を設けるようにしたものである。
【００１４】
(7)　本発明の第７の態様は、上述の第５または第６の態様に係るコンピュータシステムにおいて、
アクセス権設定手段が、照合結果が一致した場合には第１のアクセス権を設定し、照合結果が一致しなかった場合には第１のアクセス権よりも制限事項の多い第２のアクセス権を設定するようにしたものである。
【００１５】
(8)　本発明の第８の態様は、上述の第５～第７の態様に係るコンピュータシステムにおいて、
クライアントコンピュータに付与されたＩＰアドレス、クライアントコンピュータに設定されたデフォルトゲートウエイアドレス、クライアントコンピュータに設定されたプロキシサーバアドレス、もしくは、クライアントコンピュータが利用するＤＮＳサーバによって照会可能なドメイン名を、当該クライアントコンピュータのネットワーク環境を示す環境情報として用いるようにしたものである。
【００１６】
(9)　本発明の第９の態様は、ネットワーク網と、このネットワーク網に接続されたサーバコンピュータと、このネットワーク網に接続可能な複数のクライアントコンピュータと、このクライアントコンピュータに接続して用いるために個々のユーザに発行された携帯可能情報記録媒体と、を備えるコンピュータシステムにおいて、
各クライアントコンピュータに、それぞれ他のクライアントコンピュータと識別可能な固有の識別コードを記録しておき、

各携帯可能情報記録媒体に、それぞれ特定のクライアントコンピュータに記録されている特定の識別コードに対応する識別コードと、それぞれクライアントコンピュータをネットワーク網の特定箇所に接続した場合に得られる特定のネットワーク環境を示す環境情報と、を記録しておき、

各クライアントコンピュータには、携帯可能情報記録媒体を接続するためのインターフェイス手段と、現在接続中の携帯可能情報記録媒体に記録されている識別コードと自分自身に記録されている識別コードとを照合する識別コード照合手段と、現在接続中の携帯可能情報記録媒体に記録されている環境情報によって示されるネットワーク環境と自分自身の現在のネットワーク環境とを照合する環境照合手段と、これらの照合結果に基づいて所定のアクセス権を設定するアクセス権設定手段と、設定されたアクセス権の範囲内でサーバコンピュータに対するアクセスを行うサーバアクセス手段と、を設けるようにしたものである。

【００１７】

(10)　本発明の第１０の態様は、ネットワーク網と、このネットワーク網に接続されたサーバコンピュータと、このネットワーク網に接続可能な複数のクライアントコンピュータと、このクライアントコンピュータに接続して用いるために個々のユーザに発行された携帯可能情報処理装置と、を備えるコンピュータシステムにおいて、

各クライアントコンピュータに、それぞれ他のクライアントコンピュータと識別可能な固有の識別コードを記録しておき、

各携帯可能情報処理装置に、それぞれ特定のクライアントコンピュータに記録されている特定の識別コードに対応する識別コードと、それぞれクライアントコンピュータをネットワーク網の特定箇所に接続した場合に得られる特定のネットワーク環境を示す環境情報と、を記録しておき、

各クライアントコンピュータには、携帯可能情報処理装置を接続するためのインターフェイス手段と、現在接続中の携帯可能情報処理装置から伝達されてきたアクセス権の範囲内でサーバコンピュータに対するアクセスを行うサーバアクセス手段と、を設け、

携帯可能情報処理装置には、現在接続中のクライアントコンピュータに記録されている識別コードと自分自身に記録されている識別コードとを照合する識別コード照合手段と、現在接続中のクライアントコンピュータのネットワーク環境と自分自身に記録されている環境情報によって示されるネットワーク環境とを照合する環境照合手段と、これらの照合結果に基づいて所定のアクセス権を設定するアクセス権設定手段と、設定されたアクセス権を現在接続中のクライアントコンピュータに伝達するアクセス権伝達手段と、を設けるようにしたものである。

【００１８】

(11)　本発明の第１１の態様は、上述の第９または第１０の態様に係るコンピュータシステムにおいて、

アクセス権設定手段が、識別コード照合手段による照合結果が一致した場合には第１のアクセス権を設定し、識別コード照合手段による照合結果は一致しないが環境照合手段による照合結果が一致した場合には第１のアクセス権よりも制限事項の多い第２のアクセス権を設定し、いずれの照合結果も一致しなかった場合には第２のアクセス権よりも更に制限事項の多い第３のアクセス権を設定するようにしたものである。

【００１９】

(12)　本発明の第１２の態様は、上述の第９または第１０の態様に係るコンピュータシステムにおいて、

アクセス権設定手段が、識別コード照合手段による照合結果と環境照合手段による照合結果との双方が一致した場合には第１のアクセス権を設定し、識別コード照合手段による照合結果は一致したが環境照合手段による照合結果は一致しない場合には第１のアクセス権よりも制限事項の多い第２のアクセス権を設定し、いずれの照合結果も一致しなかった場合には第２のアクセス権よりも更に制限事項の多い第３のアクセス権を設定するようにしたものである。

【００２０】
(13)　本発明の第１３の態様は、ネットワーク網と、このネットワーク網に接続されたサーバコンピュータと、このネットワーク網に接続可能な複数のクライアントコンピュータと、を備えるコンピュータシステムについて、個々のユーザがクライアントコンピュータを利用してサーバコンピュータへアクセスする際のアクセス権を設定する方法において、
個々のユーザに対して、クライアントコンピュータに接続して用いるための携帯可能情報処理装置を発行し、この携帯可能情報処理装置に、特定のクライアントコンピュータに記録されている識別コードであって当該特定のクライアントコンピュータを他のクライアントコンピュータと識別することが可能な固有の識別コードに対応する識別コードを記録しておく準備段階と、
ユーザが、自分に対して発行された所定の携帯可能情報処理装置を所定のクライアントコンピュータに接続し、当該所定のクライアントコンピュータに対する利用開始手続を行ったときに、当該所定のクライアントコンピュータもしくは当該所定の携帯可能情報処理装置によって、当該所定のクライアントコンピュータに記録されている識別コードと当該所定の携帯可能情報処理装置に記録されている識別コードとを照合させ、この照合結果に基づいて所定のアクセス権を設定させるアクセス権設定段階と、
を行い、アクセス権設定段階において、照合結果が一致しなかった場合には、照合結果が一致した場合に比べて、制限事項の多いアクセス権の設定を行うようにしたものである。

【００２１】
(14)　本発明の第１４の態様は、ネットワーク網と、このネットワーク網に接続されたサーバコンピュータと、このネットワーク網に接続可能な複数のクライアントコンピュータと、を備えるコンピュータシステムについて、個々のユーザがクライアントコンピュータを利用してサーバコンピュータへアクセスする際のアクセス権を設定する方法において、
個々のユーザに対して、クライアントコンピュータに接続して用いるための携帯可能情報処理装置を発行し、この携帯可能情報処理装置に、クライアントコンピュータをネットワーク網の特定箇所に接続した場合に得られる特定のネットワーク環境を示す環境情報を記録しておく準備段階と、
ユーザが、自分に対して発行された所定の携帯可能情報処理装置を所定のクライアントコンピュータに接続し、当該所定のクライアントコンピュータに対する利用開始手続を行ったときに、当該所定のクライアントコンピュータもしくは当該所定の携帯可能情報処理装置によって、当該所定のクライアントコンピュータの現在のネットワーク環境と当該所定の携帯可能情報処理装置に記録されている環境情報によって示されるネットワーク環境とを照合させ、この照合結果に基づいて所定のアクセス権を設定させるアクセス権設定段階と、
を行い、アクセス権設定段階において、照合結果が一致しなかった場合には、照合結果が一致した場合に比べて、制限事項の多いアクセス権の設定を行うようにしたものである。

【００２２】
(15)　本発明の第１５の態様は、ネットワーク網と、このネットワーク網に接続されたサーバコンピュータと、このネットワーク網に接続可能な複数のクライアントコンピュータと、を備えるコンピュータシステムについて、個々のユーザがクライアントコンピュータを利用してサーバコンピュータへアクセスする際のアクセス権を設定する方法において、
個々のユーザに対して、クライアントコンピュータに接続して用いるための携帯可能情報処理装置を発行し、この携帯可能情報処理装置に、特定のクライアントコンピュータに記録されている識別コードであって当該特定のクライアントコンピュータを他のクライアントコンピュータと識別することが可能な固有の識別コードに対応する識別コードと、ク

ライアントコンピュータをネットワーク網の特定箇所に接続した場合に得られる特定のネットワーク環境を示す環境情報と、を記録しておく準備段階と、

ユーザが、自分に対して発行された所定の携帯可能情報処理装置を所定のクライアントコンピュータに接続し、当該所定のクライアントコンピュータに対する利用開始手続を行ったときに、当該所定のクライアントコンピュータもしくは当該所定の携帯可能情報処理装置によって、当該所定のクライアントコンピュータに記録されている識別コードと当該所定の携帯可能情報処理装置に記録されている識別コードとを照合させるとともに、当該所定のクライアントコンピュータの現在のネットワーク環境と当該所定の携帯可能情報処理装置に記録されている環境情報によって示されるネットワーク環境とを照合させ、これらの照合結果に基づいて所定のアクセス権を設定させるアクセス権設定段階と、

を行い、アクセス権設定段階において、識別コードの照合結果が一致した場合には第１のアクセス権を設定し、識別コードの照合結果は一致しないがネットワーク環境の照合結果が一致した場合には第１のアクセス権よりも制限事項の多い第２のアクセス権を設定し、いずれの照合結果も一致しなかった場合には第２のアクセス権よりも更に制限事項の多い第３のアクセス権を設定するようにしたものである。

【００２３】

(16)　本発明の第１６の態様は、ネットワーク網と、このネットワーク網に接続されたサーバコンピュータと、このネットワーク網に接続可能な複数のクライアントコンピュータと、を備えるコンピュータシステムについて、個々のユーザがクライアントコンピュータを利用してサーバコンピュータへアクセスする際のアクセス権を設定する方法において、

個々のユーザに対して、クライアントコンピュータに接続して用いるための携帯可能情報処理装置を発行し、この携帯可能情報処理装置に、特定のクライアントコンピュータに記録されている識別コードであって当該特定のクライアントコンピュータを他のクライアントコンピュータと識別することが可能な固有の識別コードに対応する識別コードと、クライアントコンピュータをネットワーク網の特定箇所に接続した場合に得られる特定のネットワーク環境を示す環境情報と、を記録しておく準備段階と、

ユーザが、自分に対して発行された所定の携帯可能情報処理装置を所定のクライアントコンピュータに接続し、当該所定のクライアントコンピュータに対する利用開始手続を行ったときに、当該所定のクライアントコンピュータもしくは当該所定の携帯可能情報処理装置によって、当該所定のクライアントコンピュータに記録されている識別コードと当該所定の携帯可能情報処理装置に記録されている識別コードとを照合させるとともに、当該所定のクライアントコンピュータの現在のネットワーク環境と当該所定の携帯可能情報処理装置に記録されている環境情報によって示されるネットワーク環境とを照合させ、これらの照合結果に基づいて所定のアクセス権を設定させるアクセス権設定段階と、

を行い、アクセス権設定段階において、識別コード照合手段による照合結果と環境照合手段による照合結果との双方が一致した場合には第１のアクセス権を設定し、識別コード照合手段による照合結果は一致したが環境照合手段による照合結果は一致しない場合には第１のアクセス権よりも制限事項の多い第２のアクセス権を設定し、いずれの照合結果も一致しなかった場合には第２のアクセス権よりも更に制限事項の多い第３のアクセス権を設定するようにしたものである。

【００２４】

(17)　本発明の第１７の態様は、上述の第１～第１２の態様に係るコンピュータシステムにおけるクライアントコンピュータとしてコンピュータを機能させるためのプログラムを用意し、当該プログラムをコンピュータ読み取り可能な記録媒体に記録して配付できるようにしたものである。

【発明の効果】

【００２５】

本発明に係るコンピュータシステムによれば、ユーザが利用しているクライアントコンピュータが、当該ユーザのために用意された特定のクライアントコンピュータであるか否

か、あるいは、当該ユーザのために用意された特定のネットワーク環境にあるか否か、を認識することにより、アクセス権の設定を行うことができるので、個々のユーザに対して、状況に応じて異なるアクセス権を設定することが可能になる。

【発明を実施するための最良の形態】

【００２６】

以下、本発明を図示する実施形態に基づいて説明する。

【００２７】

＜＜＜　§０．本発明を導入する背景　＞＞＞

はじめに、図１に示す例を参考にして、本発明を導入する背景を説明する。図１は、ネットワーク網１００に、２台のサーバコンピュータ１１０，１２０と、８台のクライアントコンピュータ１１，１２，１３，１４，２１，２２，２３，３１とを接続して構成されるコンピュータシステムのモデルを示すブロック図である。一般的な企業で利用されているコンピュータシステムでは、より多数のサーバコンピュータや、より多数のクライアントコンピュータが用いられるのが普通であるが、ここでは便宜上、図示した単純なモデルについて説明を行うことにする。

【００２８】

ネットワーク網１００は、通常、多数のルータやその間を接続する種々の回線によって構成される。一般に、ネットワークの形態としては、ＬＡＮ，ＷＡＮ，インターネットなど、様々な形態があるが、ネットワーク網１００はどのような形態で構成してもかまわない。また、図では、ネットワーク網１００と各クライアントコンピュータとの間を線で接続して示しているが、これらの間は必ずしも有線接続する必要はなく、無線ＬＡＮを用いてもかまわない。

【００２９】

ここでは、説明の便宜上、このコンピュータシステムが、ある１つの企業で利用されているシステムであるものとし、クライアントコンピュータ１１，１２，１３，１４は、この企業の人事部１０に設置されており、クライアントコンピュータ２１，２２，２３は、この企業の談話室２０に設置されており、クライアントコンピュータ３１は、この企業の社員寮３０の一室に設置されているものとする。更に、人事部に所属する１人の社員をユーザ甲と呼ぶことにし、人事部１０内のユーザ甲のデスクの上には、クライアントコンピュータ１１が設置されているものとしよう。すなわち、ユーザ甲には、会社からクライアントコンピュータ１１が支給されており、ユーザ甲は、自分のデスクに向かいながら、クライアントコンピュータ１１を操作することにより、日常業務を遂行することになる。

【００３０】

一方、サーバコンピュータ１１０，１２０には、この会社の業務上の様々なデータが蓄積されており、個々の社員は、必要に応じて、クライアントコンピュータからサーバコンピュータ１１０，１２０へとアクセスし、必要なデータの読出し、書き込み、改変などの処理を行うことになる。ここでは、説明の便宜上、サーバコンピュータ１１０には、全社員に対してアクセスを許可すべき汎用業務データが保存されており、サーバコンピュータ１２０には、特定の部署に所属する社員に対してのみアクセスさせるべき機密性の高い専用業務データが保存されているものとしよう。

【００３１】

もちろん、このようなコンピュータシステムを運用する上では、セキュリティの管理が重要である。従来の一般的なセキュリティ管理方法では、個々の社員に、その所属や職責に応じて、それぞれ固有のアクセス権を設定するような運用が行われる。上述の例の場合、人事部員であるユーザ甲には、たとえば、サーバコンピュータ１１０内の汎用業務データに対する読出しを許可するアクセス権と、サーバコンピュータ１２０内の人事部専用業務データに対する読出し／書き込みを許可するアクセス権とが設定される。

【００３２】

このように、ユーザごとのアクセス権管理を行うには、通常、個々のユーザにそれぞれ所定のアカウント（ユーザ名）とパスワードを付与し、個々のアカウントについてそれぞ

れ所定のアクセス権の設定を行っておき、特定のアカウントによるログイン手続があった場合には、パスワードの照合によりこのログイン手続が正規のものであることを確認した後、当該アカウントに設定されているアクセス権の範囲内でアクセスを許可する、という運用が行われる。たとえば、上述の例では、人事部員であるユーザ甲が、自分のデスクの上に設置されているクライアントコンピュータ１１を起動して利用開始の手続を行うと、所定のアカウントとパスワードを入力する操作を要求されることになる。ここで入力したアカウントとパスワードが正規のものとして認証されると、以後は、予めユーザ甲に設定されているアクセス権の範囲内で、サーバコンピュータ１１０，１２０に対するアクセスが可能になる。

【００３３】

従来から行われている一般的なセキュリティ管理の手法は、上述の例のように、個々のユーザごとに特定のアクセス権を設定する、という基本方針に基づくものである。もちろん、個々の社員（ユーザ）が常に誠実に業務を遂行するであろうという前提に立てば、このような基本方針に基づくセキュリティ管理は非常に合理的である。しかしながら、多数の社員をかかえる企業では、社員の不正行為の可能性も考慮して、セキュリティ管理を行う必要がある。

【００３４】

たとえば、人事部員の暗黙の了解事項として、「個々の社員の給与明細を他の部署の者に見せてはならない」という規則があったとしよう。上述の例では、人事部員であるユーザ甲には、サーバコンピュータ１２０内の人事部専用業務データへのアクセス権が与えられているので、ユーザ甲は、自分のデスクの上のクライアントコンピュータ１１の画面上に、個々の社員の給与明細を表示させ、その場で閲覧することは可能である。しかしながら、そのような状況下では、上記暗黙の了解事項を破るような行為が行われる可能性は低いであろう。少なくとも、クライアントコンピュータ１１が設置された部屋には、人事部の他のスタッフも詰めており、上司による監督も行われているであろうから、他の部署の友人を自分のデスクの脇まで呼んできて、クライアントコンピュータ１１上に表示させた給与明細を閲覧させる、というような行為を敢えて行うとは考えにくい。

【００３５】

ところが、このユーザ甲が、談話室２０で友人と休憩している場合を考えると、状況は一転することが理解できよう。もし、ユーザ甲が、談話室２０に設置されているクライアントコンピュータ２１を利用してログインした場合にも、ユーザ甲としてのアクセス権がそのまま与えられるとすれば、談話室２０に設置されているクライアントコンピュータ２１の画面上にも、個々の社員の給与明細を表示させることが可能になる。談話室２０では、上司の目も届かないので、規則に反して、給与明細の情報を友人に閲覧させてしまう可能性は高い。更に、このユーザ甲が、社員寮３０の自室に帰宅し、この自室に設置されたクライアントコンピュータ３１を利用してログインした場合にも、ユーザ甲としてのアクセス権がそのまま与えられるとすれば、規則が破られる可能性は更に高くなるであろう。

【００３６】

クライアントコンピュータの設置環境によって、規則違反が行われる可能性が高くなる例は、この他にも、枚挙にいとまがない。たとえば、「人事部員は、人事部長の許可がなければ、人事部専用業務データを外部の記録媒体に保存したりプリントアウトしてはならない」というような社内規則があったとしよう。この社内規則によれば、人事部員は、サーバコンピュータ１２０内の人事部専用業務データにアクセスすることは可能であるが、このデータを許可なくフロッピディスクやＣＤ－Ｒに保存したり、プリントしたりすることは禁止される。したがって、人事部１０に配置されたクライアントコンピュータ１１～１４を用いて、このような規則に反する行為が行われる可能性は低い。フロッピディスクに保存する行為やプリントアウトする行為は、上司や他のスタッフの目に触れやすいため、罪悪感により、違反行為は自粛されることになろう。しかしながら、談話室２０に配置されたクライアントコンピュータ２１～２３や、社員寮３０に配置されたクライアントコンピュータ３１を用いた場合は事情が異なってくる。

【００３７】
また、機密性を重んじる部署では、当該部署の出入り口に監視カメラを設置したり、出入りの際に保守要員によるチェックを義務づけたりするケースもある。このような部署では、たとえ機密データをフロッピディスクやＣＤ－Ｒに保存したり、プリントアウトしたりしても、それを部署外に持ち出すことが困難であるため、規則違反が行われる可能性は低い。ところが、社員寮３０に設置されたクライアントコンピュータ３１を利用した場合にも、同じアクセス権が与えられるとすると、当該部署の出入りを厳しくしても、セキュリティ上の意味はなくなってしまう。

【００３８】
もちろん、このようなセキュリティ上の問題を解決する手法として、通常、ファイアウォールを構築する方法が採られている。たとえば、図１に示す例の場合、ネットワーク網１００内に多数のルータを組み込んで、個々のエリアごとにファイアウオールを構築し、サーバコンピュータ１２０に対して、ノードＮ２やＮ３を経由したアクセスがあった場合には、これを拒絶する、というような運用を行えば、上述のような不正行為を防ぐことは可能である。しかしながら、そのためには、どこにどのようなファイアウオールを設置するか、というネットワーク網に関する複雑な設定が必要になる。本発明は、以下に述べる別なアプローチにより、このようなセキュリティ上の問題を解決するものである。

【００３９】
＜＜＜　§１．本発明の第１の実施形態　＞＞＞
図２は、本発明の第１の実施形態を説明するためのブロック図であり、図１に示すコンピュータシステムの一部を示すものである。この第１の実施形態の基本概念は、個々のユーザについて、それぞれ本来のクライアントコンピュータを定めておき、各ユーザが、本来のクライアントコンピュータを用いてアクセスしてきた場合には、当該ユーザに設定されている本来のアクセス権によるアクセスを許可するが、それ以外のクライアントコンピュータを用いてアクセスしてきた場合には、当該ユーザに設定されている本来のアクセス権よりも制限事項の多いアクセス権によるアクセスしか許可しないようにする、という運用にある。

【００４０】
いま、一例として、３人のユーザ甲，乙，丙がこのコンピュータシステムを利用する場合を考える。ここでは、ユーザ甲および乙は、いずれも人事部員であるものとし、ユーザ丙は、談話室を管理する庶務課員であるものとしよう。また、ユーザ甲には、本来のクライアントコンピュータとしてコンピュータ１１が支給されており、ユーザ乙には、本来のクライアントコンピュータとしてコンピュータ１２が支給されており、ユーザ丙には、本来のクライアントコンピュータとしてコンピュータ２１が支給されているものとする。図１に示すように、ユーザ甲，乙に支給されたクライアントコンピュータ１１，１２は、人事部１０の部屋に設置されており、ユーザ丙に支給されたクライアントコンピュータ２１は、談話室２０に設置されている。

【００４１】
本発明に係るコンピュータシステムおけるセキュリティ管理を行うためには、個々のユーザに対して、クライアントコンピュータに接続して用いるための携帯可能情報記録媒体が発行される。図２には、３人のユーザ甲，乙，丙に対して、それぞれ携帯可能情報記録媒体Ｒ１１，Ｒ１２，Ｒ２１が発行された例が示されている。この携帯可能情報記録媒体Ｒ１１，Ｒ１２，Ｒ２１は、各ユーザが容易に携帯することが可能であり、データを記録する機能をもった媒体であれば、どのようなものでもかまわない。ただ、実用上は、記録されたデータに対する十分なセキュリティを確保することが可能な媒体を用いるのが好ましい。具体的には、ＩＣカードを携帯可能情報記録媒体として用いるのが最適である。ＩＣカードは、携帯性に優れており、また、記録されているデータに対して十分なセキュリティを確保することが可能である。

【００４２】
なお、携帯可能情報記録媒体は、本発明に利用するための専用の媒体である必要はなく

、他の用途と兼用することも可能である。たとえば、最近では、ＩＣカードを利用した社員証などを各社員に発行する企業も増えてきているが、そのような場合は、社員証を携帯可能情報記録媒体として利用すれば足りる。ここでは、図２に示す携帯可能情報記録媒体Ｒ１１，Ｒ１２，Ｒ２１が、それぞれユーザ甲，乙，丙に対して発行されたＩＣカードからなる社員証であるものとして、以下の説明を行うことにする。

【００４３】

この第１の実施形態では、個々の携帯可能情報記録媒体Ｒ１１，Ｒ１２，Ｒ２１に、それぞれ特定のクライアントコンピュータの識別コードを記録しておく。ここで、特定のクライアントコンピュータとは、各ユーザが利用すべき本来のコンピュータである。図２に示す例の場合、ユーザ甲に発行された携帯可能情報記録媒体Ｒ１１（ユーザ甲の社員証として発行されたＩＣカード）には、ユーザ甲が本来利用すべきクライアントコンピュータ１１の識別コードＩＤ（１１）が記録されている。同様に、ユーザ乙に発行された携帯可能情報記録媒体Ｒ１２（ユーザ乙の社員証として発行されたＩＣカード）には、ユーザ乙が本来利用すべきクライアントコンピュータ１２の識別コードＩＤ（１２）が記録されており、ユーザ丙に発行された携帯可能情報記録媒体Ｒ２１（ユーザ丙の社員証として発行されたＩＣカード）には、ユーザ丙が本来利用すべきクライアントコンピュータ２１の識別コードＩＤ（２１）が記録されている。

【００４４】

クライアントコンピュータの識別コードとしては、当該クライアントコンピュータ内のいずれかの部分に記録されている識別コードであって、当該クライアントコンピュータを他のクライアントコンピュータと識別することが可能な固有の識別コードであれば、どのようなコードを用いてもかまわない。

【００４５】

たとえば、クライアントコンピュータに内蔵されているＬＡＮ通信回路に付与されたＭＡＣアドレス（Media Access Control Address）を、本発明における識別コードとして利用することができる。各クライアントコンピュータには、ネットワーク網１００に接続するためのＬＡＮ通信回路が備わっている。現在、標準的に用いられているイーサネット用のＬＡＮ通信回路には、個々のメーカーが設定したユニークなＭＡＣアドレスが付与されている。しかも、このＭＡＣアドレスは、ＬＡＮ通信回路内のＩＣチップに記録されており、必要があれば、クライアントコンピュータのＯＳの機能を用いて読み出すことが可能である。したがって、このＭＡＣアドレスを識別コードとして用いれば、すべてのクライアントコンピュータを相互に識別することが可能になる。この場合、ユーザ甲の社員証として発行された携帯可能情報記録媒体Ｒ１１には、クライアントコンピュータ１１に内蔵されているＬＡＮ通信回路のＭＡＣアドレスを、識別コードＩＤ（１１）として記録しておけばよい。

【００４６】

もちろん、本発明における識別コードとして利用できるコードは、ＭＡＣアドレスに限定されるものではなく、クライアントコンピュータの記憶装置に格納されている何らかの固有データであれば、ＭＡＣアドレスと同様に識別コードとして利用することが可能である。たとえば、個々のクライアントコンピュータごとに、それぞれユニークなシリアル番号が付与されており、このシリアル番号が、各クライアントコンピュータの内部に何らかの形で記録されていれば、当該シリアル番号を識別コードとして用いることも可能である。あるいは、意図的に、各クライアントコンピュータのハードディスクの特定領域に、それぞれユニークなシリアル番号を書き込んでおき、これを識別コードとして用いることも可能である。

【００４７】

また、各クライアントコンピュータの記憶装置に格納されているアプリケーションプログラムの構成を示す情報を、当該クライアントコンピュータを識別するための固有の識別コードとして用いることも可能である。通常、各クライアントコンピュータには、その業務に応じてそれぞれ所定のアプリケーションプログラムがインストールされるので、特定

のアプリケーションプログラムがインストールされているという事実を、識別コードとして利用することも可能である。もっとも、実際には、同一種類のアプリケーションプログラムがインストールされたコンピュータが多数存在することも少なくないので、その場合には、アプリケーションプログラムのインストール時に入力したシリアル番号を、アプリケーションプログラムの構成を示す情報とし、識別コードとして利用すればよい。すなわち、一般的なアプリケーションプログラムでは、インストール時に所定のシリアル番号の入力が求められ、入力したシリアル暗号は、ハードディスク装置などに記録されることが多い。そこで、このアプリケーションプログラム用のシリアル番号を識別コードとして利用しても、個々のクライアントコンピュータを相互に区別することが可能である。

【００４８】

さて、図２に示す例のように、各ユーザ甲，乙，丙に対して発行した携帯可能情報記録媒体Ｒ１１，Ｒ１２，Ｒ２１に、それぞれ特定のクライアントコンピュータの識別コードを記録する準備段階が完了したら、このコンピュータシステムの運用を開始することが可能になる。このコンピュータシステムでは、各ユーザは、それぞれ支給されたクライアントコンピュータを利用する際に、社員証として発行されたＩＣカード、すなわち、携帯可能情報記録媒体を当該クライアントコンピュータに接続する作業を行うことが要求される。たとえば、ユーザ甲は、自分のデスクの上でクライアントコンピュータ１１を利用する際に、社員証として発行されたＩＣカードである携帯可能情報記録媒体Ｒ１１を、クライアントコンピュータ１１に接続して、所定の利用開始手続（一般に、ログイン手続あるいはログオン手続と呼ばれている手続）を行う必要がある。したがって、この実施形態では、各クライアントコンピュータには、ＩＣカード用のリーダライタ装置が装備されている。

【００４９】

本実施形態に係るコンピュータシステムにおけるセキュリティ管理の基本原理は、ユーザが、自分に対して発行された所定の携帯可能情報記録媒体を所定のクライアントコンピュータに接続し、当該所定のクライアントコンピュータに対する利用開始手続を行ったときに、当該所定のクライアントコンピュータに記録されている識別コードと当該所定の携帯可能情報記録媒体に記録されている識別コードとを照合させ、この照合結果に基づいて所定のアクセス権を設定させる点にある。より具体的には、照合結果が一致しなかった場合には、照合結果が一致した場合に比べて、制限事項の多いアクセス権の設定を行うようにする。

【００５０】

たとえば、図２に示す例において、ユーザ甲が、自己の社員証として発行された携帯可能情報記録媒体Ｒ１１を、人事部１０に設置された本来使用すべきクライアントコンピュータ１１に接続して利用開始手続を行った場合、クライアントコンピュータ１１に記録されている識別コードＩＤ（１１）と携帯可能情報記録媒体Ｒ１１に記録されている識別コードＩＤ（１１）との照合作業が行われる。そして、この照合結果に基づいてアクセス権が設定される。この例の場合、照合結果は一致するので、クライアントコンピュータ１１を利用したユーザ甲のアクセス行為に対しては、ユーザ甲に設定された本来のアクセス権が与えられることになる。たとえば、ユーザ甲には、サーバコンピュータ１１０内の汎用業務データに対する読出しを許可するアクセス権と、サーバコンピュータ１２０内の人事部専用業務データに対する読出し／書き込みを許可するアクセス権とが与えられる。

【００５１】

一方、ユーザ甲が、談話室２０に設置されたクライアントコンピュータ２１を利用したアクセスを行った場合を考えてみよう。この場合、ユーザ甲は、携帯可能情報記録媒体Ｒ１１を、クライアントコンピュータ２１に接続して利用開始手続を行うことになるが、クライアントコンピュータ２１に記録されている識別コードＩＤ（２１）と携帯可能情報記録媒体Ｒ１１に記録されている識別コードＩＤ（１１）とは一致しないので、この場合は、照合結果が一致した場合に比べて、制限事項の多いアクセス権の設定が行われる。たとえば、サーバコンピュータ１１０内の汎用業務データに対する読出しは許可されるが、サ

ーバコンピュータ１２０内の人事部専用業務データに対するアクセスは一切禁止されるようなアクセス権が与えられる。

【００５２】

このような運用を行えば、結局、各ユーザには、予め定められた本来のクライアントコンピュータを利用している場合には、本来のアクセス権が与えられることになるが、それ以外のクライアントコンピュータを利用している場合には、ユーザのアクセス権は制限されることになる。上述の例の場合、人事部員であるユーザ甲は、人事部１０に設置されたクライアントコンピュータ１１で作業する限りは、人事部員に与えられる本来のアクセス権をもって各サーバコンピュータへのアクセスが可能になるが、談話室２０や社員寮３０に設置されたクライアントコンピュータを利用した場合は、本来のアクセス権を取得することはできない。したがって、§０で述べたようなセキュリティ上の問題を解決することができる。

【００５３】

ところで、識別コードの照合処理や、照合結果に応じたアクセス権の設定処理を行うためには、クライアントコンピュータ内にそれなりの構成要素を用意しておく必要がある。図３は、この第１の実施形態を行うためのクライアントコンピュータ１１の構成を示すブロック図である。図示のとおり、クライアントコンピュータ１１には、サーバアクセス手段１１Ａ，アクセス権設定手段１１Ｂ，識別コード照合手段１１Ｃ，インターフェイス手段１１Ｄが設けられている。もちろん、クライアントコンピュータ１１には、この他にも、クライアントコンピュータとしての機能を果たすための種々の構成要素（たとえば、ＯＳプログラムやアプリケーションプログラムを実行するためのＣＰＵ、メモリ、ハードディスクや、入出力装置など）が備わっているが、ここでは説明は省略する。

【００５４】

前述したとおり、このクライアントコンピュータ１１には、他のクライアントコンピュータと識別可能な固有の識別コードＩＤ（１１）が記録されている。たとえば、ＭＡＣアドレスを識別コードＩＤ（１１）として利用するようにすれば、識別コードＩＤ（１１）はもともとクライアントコンピュータ１１内に組み込まれていることになるので、識別コードをクライアントコンピュータ１１に書き込むような作業は一切不要である。一方、携帯可能情報記録媒体Ｒ１１にも、識別コードＩＤ（１１）が記録されている。こちらの方は、このコンピュータシステムの管理者による書き込み作業が必要になる。ここに示す例では、携帯可能情報記録媒体Ｒ１１は、ユーザ甲の社員証として発行されたＩＣカードであるため、その中には、識別コードＩＤ（１１）以外のデータも多数記録されているが、ここではそれらの説明は省略する。

【００５５】

ここで、インターフェイス手段１１Ｄは、携帯可能情報記録媒体Ｒ１１を接続するための構成要素であり、この例の場合、ＩＣカード用のリーダライタ装置によって構成されている。ユーザは、このクライアントコンピュータ１１に対する利用開始手続を行う際に、ＩＣカードとしての携帯可能情報記録媒体Ｒ１１を、リーダライタ装置としてのインターフェイス手段１１Ｄに装填することにより、両者を接続状態にすることができる。また、利用を終了する際には、このＩＣカードを、リーダライタ装置から引き抜くことにより、両者を分離することができる。

【００５６】

識別コード照合手段１１Ｃは、現在接続中の携帯可能情報記録媒体に記録されている識別コードと自分自身に記録されている識別コードとを照合する機能を有する構成要素であり、アクセス権設定手段１１Ｂは、この照合結果に基づいて所定のアクセス権を設定する機能を有する構成要素である。アクセス権設定手段１１Ｂは、照合結果が一致した場合には第１のアクセス権を設定し、照合結果が一致しなかった場合にはこの第１のアクセス権よりも制限事項の多い第２のアクセス権を設定することになる。サーバアクセス手段１１Ａは、設定されたアクセス権の範囲内で、サーバコンピュータ１１０，１２０に対するアクセスを行う構成要素である。

【００５７】
図示の例の場合、ユーザ甲が自己の社員証である携帯可能情報記録媒体Ｒ１１を用いて、クライアントコンピュータ１１への利用開始手続を行っているので、識別コード照合手段１１Ｃによる照合結果は一致する。すなわち、識別コード照合手段１１Ｃは、インターフェイス手段１１Ｄを介して読み出した携帯可能情報記録媒体Ｒ１１内の識別コードＩＤ（１１）と、クライアントコンピュータ１１内に記録されていた識別コードＩＤ（１１）とを比較照合する処理を行うことになるので、この例の場合は、両者が一致する結果が得られるので、アクセス権設定手段１１Ｂは、第１のアクセス権を設定する。
【００５８】
もし、談話室２０に設置されたクライアントコンピュータ２１に対して、同様の利用開始手続を行ったとすると、携帯可能情報記録媒体Ｒ１１内の識別コードＩＤ（１１）と、クライアントコンピュータ２１内に記録されていた識別コードＩＤ（２１）とは一致しないので、クライアントコンピュータ２１内の識別コード照合手段２１Ｃは不一致の結果を示し、アクセス権設定手段２１Ｂは、第２のアクセス権を設定することになる。
【００５９】
上述した例では、第１のアクセス権としては、サーバコンピュータ１１０内の汎用業務データに対する読出しを許可するとともに、サーバコンピュータ１２０内の人事部専用業務データに対する読出し／書き込みを許可する権利を設定し、第２のアクセス権としては、サーバコンピュータ１１０内の汎用業務データに対する読出しを許可するが、サーバコンピュータ１２０内のデータに対するアクセスは一切禁止する権利を設定することになる。
【００６０】
もっとも、このようなアクセス許否の具体的な内容設定は、必ずしもクライアントコンピュータ内のアクセス権設定手段によって行う必要はない。実用上は、むしろ、アクセス権設定手段においては、第１のアクセス権か第２のアクセス権かのいずれかを設定するだけにしておき、細かなアクセス許否の設定は、サーバコンピュータ側で行うようにするのが好ましい。たとえば、サーバコンピュータ１２０内の人事部専用業務データについては、第１のアクセス権をもったユーザ甲からのアクセスがあった場合には、読出し／書き込みを許可するが、第２のアクセス権をもったユーザ甲からのアクセスがあった場合には、一切のアクセスを拒絶する、というような設定を行っておけばよい。この場合、ユーザ甲からのアクセスであることの認証は、従来どおり、ユーザ甲に与えたアカウント名とパスワードの照合により行うようにすればよい。
【００６１】
なお、識別コードの照合処理や、照合結果に応じたアクセス権の設定処理は、必ずしもクライアントコンピュータ側で行う必要はない。すなわち、携帯可能情報記録媒体が情報処理機能を有している場合には、携帯可能情報記録媒体側でこれらの処理を実行させることも可能である。現在、社員証などに利用されているＩＣカードには、単なる情報記録媒体としての機能だけでなく、ＣＰＵを内蔵した情報処理装置としての機能も備わっている。このような情報処理機能を備えた携帯可能情報記録媒体（以下、携帯可能情報処理装置という）を用いれば、識別コードの照合処理およびアクセス権の設定処理を、携帯可能情報処理装置側で行うことが可能になる。
【００６２】
図４は、この第１の実施形態において、携帯可能情報処理装置側で照合処理およびアクセス権の設定処理を実行する変形例の構成を示すブロック図である。図示のとおり、クライアントコンピュータ１１内に、固有の識別コードＩＤ（１１）が記録されており、携帯可能情報処理装置Ｐ１１内に、このクライアントコンピュータ１１に記録されている識別コードに対応する識別コードＩＤ（１１）が記録されている点は、図３に示す例と全く同様である。ただ、クライアントコンピュータ１１には、現在接続中の携帯可能情報処理装置から伝達されてきたアクセス権の範囲内でサーバコンピュータに対するアクセスを行うサーバアクセス手段１１Ａと、携帯可能情報処理装置を接続するためのインターフェイス

手段１１Ｄと、が備わっているものの、識別コード照合手段およびアクセス権設定手段は備わっていない。

【００６３】

一方、携帯可能情報処理装置Ｐ１１は、上述したように、情報処理機能をもったＩＣカードであり、図示のとおり、識別コード照合手段１１Ｅ，アクセス権設定手段１１Ｆ，アクセス権伝達手段１１Ｇを備えている。識別コード照合手段１１Ｅは、現在接続中のクライアントコンピュータに記録されている識別コードと自分自身に記録されている識別コードとを照合する構成要素であり、アクセス権設定手段１１Ｆは、この照合結果に基づいて所定のアクセス権を設定する構成要素であり、アクセス権伝達手段１１Ｇは、設定されたアクセス権を現在接続中のクライアントコンピュータに伝達する構成要素である。

【００６４】

図示のように、ユーザ甲が自己の社員証である携帯可能情報処理装置Ｐ１１（情報処理機能をもったＩＣカード）を用いて、クライアントコンピュータ１１への利用開始手続を行うと、識別コード照合手段１１Ｅは、インターフェイス手段１１Ｄを介して読み出したクライアントコンピュータ１１内の識別コードＩＤ（１１）と、携帯可能情報処理装置Ｐ１１内に記録されていた識別コードＩＤ（１１）とを比較照合する処理を行うことになる。この例の場合は、両者が一致する結果が得られるので、アクセス権設定手段１１Ｆは、第１のアクセス権を設定し、設定したアクセス権は、インターフェイス手段１１Ｄを介して、サーバアクセス手段１１Ａへと伝えられる。その結果、サーバアクセス手段１１Ａは、第１のアクセス権に基づいてサーバコンピュータへのアクセスを行うことになる。

【００６５】

もちろん、談話室２０に設置されたクライアントコンピュータ２１に対して、同様の利用開始手続を行ったとすると、携帯可能情報処理装置Ｐ１１内の識別コードＩＤ（１１）と、クライアントコンピュータ２１内に記録されていた識別コードＩＤ（２１）とは一致しないので、識別コード照合手段１１Ｅでは、不一致の照合結果が得られることになり、アクセス権設定手段１１Ｆは、第２のアクセス権を設定する。その結果、サーバアクセス手段１１Ａは、第２のアクセス権に基づいてサーバコンピュータへのアクセスを行うことになる。

【００６６】

＜＜＜　§２．本発明の第２の実施形態　＞＞＞

図５は、本発明の第２の実施形態を説明するためのブロック図であり、図１に示すコンピュータシステムの一部を示すものである。この第２の実施形態の基本概念は、個々のユーザについて、それぞれ本来のクライアントコンピュータを定める代わりに、本来のネットワーク環境を定めておき、各ユーザが、本来のネットワーク環境に接続されたクライアントコンピュータを用いてアクセスしてきた場合には、当該ユーザに設定されている本来のアクセス権によるアクセスを許可するが、それ以外のネットワーク環境に接続されたクライアントコンピュータを用いてアクセスしてきた場合には、当該ユーザに設定されている本来のアクセス権よりも制限事項の多いアクセス権によるアクセスしか許可しないようにする、という運用にある。

【００６７】

すなわち、上述した第１の実施形態では、各ユーザが予め定められた特定のクライアントコンピュータからアクセスしているか否かに応じて異なるアクセス権の設定を行っていたのに対して、この第２の実施形態では、各ユーザが予め定められた特定のネットワーク環境からアクセスしているか否かに応じて異なるアクセス権の設定を行うことになる。ここで、ネットワーク環境とは、クライアントコンピュータをネットワーク網１００の特定箇所に接続した場合に得られる環境を意味するものであり、たとえば、図１に示す例において、ネットワーク網１００のノードＮ１を経由してサーバコンピュータ１１０，１２０へのアクセスを行うクライアントコンピュータ１１～１４と、ノードＮ２を経由してサーバコンピュータ１１０，１２０へのアクセスを行うクライアントコンピュータ２１～２３と、ノードＮ３を経由してサーバコンピュータ１１０，１２０へのアクセスを行うクライ

アントコンピュータ３１とは、いずれもネットワーク環境が異なるコンピュータということになる。

【００６８】

もっとも、ネットワーク環境は、あくまでもネットワーク網１００に対する接続環境を示すものであり、個々のクライアントコンピュータと直接関連するものではない。たとえば、図１に示す談話室２０に設置されているクライアントコンピュータ２３を、談話室２０内のＬＡＮから取り外し、人事部１０へと移動し、人事部１０のＬＡＮに接続したとすると、同一のクライアントコンピュータ２３でありながら、ネットワーク環境は変わってしまうことになる。逆に、人事部１０に設置されているクライアントコンピュータ１１が故障したため、同一の設置場所において、これを新品のクライアントコンピュータ１５に取り換えた場合、クライアントコンピュータ自身は異なるものになるが、ネットワーク環境に変化はない。

【００６９】

前述した第１の実施形態の場合、個々のクライアントコンピュータに固有のＭＡＣアドレスなどを識別コードとして用いると、コンピュータを新品に入れ替えたような場合、識別コードも変わってしまうことになる。その場合、携帯可能情報記録媒体に記録した識別コードも新たなものに書き換える作業が必要になる。ここで述べる第２の実施形態の場合、クライアントコンピュータ自身の同一性ではなく、ネットワーク環境の同一性を判断して、アクセス権の設定が行われるため、ネットワーク環境の同一性が確保されている限り、コンピュータを入れ替えたとしても、携帯可能情報記録媒体への記録内容を書き換えるような作業は必要ない。

【００７０】

図５には、３人のユーザ甲，乙，丙に対して、この第２の実施形態に基づいて、それぞれ携帯可能情報記録媒体Ｒ１１，Ｒ１２，Ｒ２１が発行された例が示されている。前述したとおり、この携帯可能情報記録媒体Ｒ１１，Ｒ１２，Ｒ２１は、それぞれユーザ甲，乙，丙に対して発行されたＩＣカードからなる社員証である。

【００７１】

この第２の実施形態では、個々の携帯可能情報記録媒体Ｒ１１，Ｒ１２，Ｒ２１に、クライアントコンピュータをネットワーク網１００の特定箇所に接続した場合に得られる特定のネットワーク環境を示す環境情報を記録しておくことになる。ここで記録される環境情報は、各ユーザが利用すべき本来のネットワーク環境を示すものになる。図５に示す例の場合、ユーザ甲に発行された携帯可能情報記録媒体Ｒ１１（ユーザ甲の社員証として発行されたＩＣカード）には、ユーザ甲が本来利用すべきネットワーク環境を示す環境情報ＥＮＶ（１１）が記録されている。具体的には、ユーザ甲が自分のデスクで利用しているクライアントコンピュータ１１についてのネットワーク環境を示す環境情報ＥＮＶ（１１）が、そのまま携帯可能情報記録媒体Ｒ１１内に記録されていることになる。同様に、ユーザ乙に発行された携帯可能情報記録媒体Ｒ１２（ユーザ乙の社員証として発行されたＩＣカード）には、ユーザ乙が本来利用すべきネットワーク環境を示す環境情報ＥＮＶ（１２）が記録されており、ユーザ丙に発行された携帯可能情報記録媒体Ｒ２１（ユーザ丙の社員証として発行されたＩＣカード）には、ユーザ丙が本来利用すべきネットワーク環境を示す環境情報ＥＮＶ（２１）が記録されている。

【００７２】

ネットワーク環境を示す環境情報としては、クライアントコンピュータをネットワーク網１００の特定箇所に接続した場合に得られる特定のネットワーク環境を示す情報であれば、どのような情報を用いてもかまわないが、以下に、環境情報として利用できる具体的な情報の例をいくつか列挙しておく。

【００７３】

たとえば、クライアントコンピュータに付与されたＩＰアドレスを環境情報として利用することが可能である。通常、企業のコンピュータシステムを構成するコンピュータには、ＤＨＣＰ（Dynamic Host Configuration Protocol）を利用して、所定のＩＰアドレス

が自動的に割り当てられる。このとき、各ネットワークのエリアごとに、それぞれ所定のアドレス範囲を定める運用が行われている場合には、ネットワーク網１００に対する接続箇所に応じて、割り当てられるアドレス範囲が異なることになる。たとえば、図１に示す例において、ネットワーク網１００のノードＮ１，Ｎ２，Ｎ３にそれぞれルータが設けられており、ノードＮ１に接続されている人事部１０のクライアントコンピュータ１１，１２，１３，１４に対しては、第１のアドレス範囲に属するＩＰアドレスが割り当てられ、ノードＮ２に接続されている談話室２０のクライアントコンピュータ２１，２２，２３に対しては、第２のアドレス範囲に属するＩＰアドレスが割り当てられ、ノードＮ３に接続されている社員寮３０のクライアントコンピュータ３１に対しては、第３のアドレス範囲に属するＩＰアドレスが割り当てられている場合、クライアントコンピュータに現時点で割り当てられているＩＰアドレスが、どのアドレス範囲に属するかを確認することにより、当該クライアントコンピュータのネットワーク環境を認識することができる。

【００７４】

たとえば、あるクライアントコンピュータに割り当てられたＩＰアドレスが第１のアドレス範囲に属するものであったとすると、当該クライアントコンピュータは、ノードＮ１に接続されている人事部１０のコンピュータであることが認識できる。ＩＰｖ４の場合、ＩＰアドレスは３２ビットの数字により表現されるが、たとえば、同一ノードに接続されるクライアントコンピュータには、上位２４ビットが同一で下位８ビットのみが異なるＩＰアドレスを付与するような規則でＩＰアドレスの決定が行われるような場合なら、ＩＰアドレスの上位２４ビットをそのままネットワーク環境を示す環境情報として利用することができる。図１に示す例の場合、たとえば、人事部１０に所属するクライアントコンピュータ１１，１２，１３，１４の各ＩＰアドレスの上位２４ビットは同一になるので、これをそのまま環境情報として利用することができる。

【００７５】

また、クライアントコンピュータに設定されたデフォルトゲートウエイアドレスを、ネットワーク環境を示す環境情報として利用することもできる。たとえば、図１に示す例において、ノードＮ１，Ｎ２，Ｎ３にそれぞれルータが設置されていたとすると、各クライアントコンピュータについて設定されるデフォルトゲートウエイアドレスは、それぞれのノードに設置されたルータのＩＰアドレスになる。たとえば、人事部１０のクライアントコンピュータ１１，１２，１３，１４には、ノードＮ１に設置されたルータのＩＰアドレスが、共通のデフォルトゲートウエイアドレスとして設定される。これに対して、談話室２０のクライアントコンピュータ２１，２２，２３には、ノードＮ２に設置されたルータのＩＰアドレスが、共通のデフォルトゲートウエイアドレスとして設定される。したがって、これらのデフォルトゲートウエイアドレスを、そのままネットワーク環境を示す環境情報として利用することができる。

【００７６】

ノードＮ１，Ｎ２，Ｎ３に、ルータではなく、プロキシサーバが設置されている場合には、クライアントコンピュータに設定されたプロキシサーバアドレスを、ネットワーク環境を示す環境情報として利用することもできる。人事部１０のクライアントコンピュータ１１，１２，１３，１４には、共通のプロキシサーバアドレスが設定されることになるが、談話室２０のクライアントコンピュータ２１，２２，２３には、それとは別な共通のプロキシサーバアドレスが設定されることになる。

【００７７】

この他、クライアントコンピュータが利用するＤＮＳサーバによって照会可能なドメイン名を、当該クライアントコンピュータのネットワーク環境を示す環境情報として用いることも可能である。ＤＮＳサーバは、ドメイン名とＩＰアドレスとを相互に変換する変換テーブル機能をもったサーバコンピュータである。図１に示す例において、もし、人事部１０に設置された各クライアントコンピュータが参照するＤＮＳサーバと、談話室２０に設置された各クライアントコンピュータが参照するＤＮＳサーバとが異なっており、それぞれの変換テーブルの内容が異なっている場合には、この差異を利用して、いずれのＤＮ

Ｓサーバを参照するクライアントコンピュータであるかを認識することが可能になる。

【００７８】

たとえば、人事部１０に設置された各クライアントコンピュータが参照するＤＮＳサーバには、「Melon」なるドメイン名をＩＰアドレスに変換するテーブルが用意されているが、談話室２０に設置された各クライアントコンピュータが参照するＤＮＳサーバには、「Melon」なるドメイン名を変換するテーブルが用意されていなかったとすれば、あるクライアントコンピュータから、「Melon」なるドメイン名を検索する操作を行い、検索が行えた場合には、当該クライアントコンピュータは、人事部１０に設置されたクライアントコンピュータであると認識することができる。

【００７９】

以上述べたとおり、クライアントコンピュータをネットワーク網１００の特定箇所に接続した場合に得られる特定のネットワーク環境を示す様々な情報を、この第２の実施形態における環境情報として利用することが可能である。ここでは、図５に示す例のように、各ユーザ甲，乙，丙に対して発行した携帯可能情報記録媒体Ｒ１１，Ｒ１２，Ｒ２１に、それぞれ特定の環境情報を記録する準備段階が完了したものとしよう。たとえば、ユーザ甲の社員証である携帯可能情報記録媒体Ｒ１１内に記録されている環境情報ＥＮＶ（１１）は、ユーザ甲が利用する本来のネットワーク環境を示す情報であり、具体的には、クライアントコンピュータ１１に付与されたＩＰアドレスの上位２４ビットであったり、ノードＮ１に設置されているルータのＩＰアドレス（デフォルトゲートウエイアドレス）であったり、ノードＮ１に設置されているプロキシサーバのアドレスであったりする。

【００８０】

図５に示す例の場合、クライアントコンピュータ１１のネットワーク環境とクライアントコンピュータ１２のネットワーク環境とは同一であり、環境情報ＥＮＶ（１１）と環境情報ＥＮＶ（１２）とは同一になる。ただし、クライアントコンピュータ２１のネットワーク環境は異なるものになるので、環境情報ＥＮＶ（２１）も異なるものになる。

【００８１】

本実施形態に係るコンピュータシステムにおけるセキュリティ管理の基本原理は、ユーザが、自分に対して発行された所定の携帯可能情報記録媒体を所定のクライアントコンピュータに接続し、当該所定のクライアントコンピュータに対する利用開始手続を行ったときに、当該所定のクライアントコンピュータの現時点でのネットワーク環境と、当該所定の携帯可能情報記録媒体に記録されている環境情報によって示されるネットワーク環境とを照合させ、この照合結果に基づいて所定のアクセス権を設定させる点にある。より具体的には、照合結果が一致しなかった場合には、照合結果が一致した場合に比べて、制限事項の多いアクセス権の設定を行うようにする。この点は、前掲の第１の実施形態と同様である。

【００８２】

たとえば、図５に示す例において、ユーザ甲が、自己の社員証として発行された携帯可能情報記録媒体Ｒ１１を、人事部１０のクライアントコンピュータ１１に接続して利用開始手続を行った場合、クライアントコンピュータ１１のネットワーク環境を示す環境情報ＥＮＶ（１１）と携帯可能情報記録媒体Ｒ１１に記録されている環境情報ＥＮＶ（１１）との照合作業が行われる。そして、この照合結果に基づいてアクセス権が設定される。この例の場合、照合結果は一致するので、クライアントコンピュータ１１を利用したユーザ甲のアクセス行為に対しては、ユーザ甲に設定された本来のアクセス権が与えられることになる。たとえば、ユーザ甲には、サーバコンピュータ１１０内の汎用業務データに対する読出しを許可するアクセス権と、サーバコンピュータ１２０内の人事部専用業務データに対する読出し／書き込みを許可するアクセス権とが与えられる。

【００８３】

ところで、図５に示す例において、クライアントコンピュータ１１のネットワーク環境とクライアントコンピュータ１２のネットワーク環境とは同一であるので、環境情報ＥＮＶ（１１）と環境情報ＥＮＶ（１２）とは同一になる。したがって、ユーザ甲が、クライ

アントコンピュータ１２を利用した場合も、上述の場合と全く同じアクセス権が与えられることになる。もちろん、クライアントコンピュータ１１を、新たなクライアントコンピュータ１５に交換し、この新たなクライアントコンピュータ１５を利用した場合も、同じアクセス権が与えられることになる。このように、ここで述べる第２の実施形態では、前述した第１の実施形態よりも自由度の高い運用が可能になる。

【００８４】

一方、ユーザ甲が、談話室２０に設置されたクライアントコンピュータ２１を利用したアクセスを行った場合は、事情が変わってくる。この場合、ユーザ甲は、携帯可能情報記録媒体Ｒ１１を、クライアントコンピュータ２１に接続して利用開始手続を行うことになるが、クライアントコンピュータ２１のネットワーク環境を示す環境情報ＥＮＶ（２１）と携帯可能情報記録媒体Ｒ１１に記録されている環境情報ＥＮＶ（１１）とは一致しないので、この場合は、照合結果が一致した場合に比べて、制限事項の多いアクセス権の設定が行われる。たとえば、サーバコンピュータ１１０内の汎用業務データに対する読出しは許可されるが、サーバコンピュータ１２０内の人事部専用業務データに対するアクセスは一切禁止されるようなアクセス権が与えられる。

【００８５】

このような運用を行えば、結局、各ユーザには、予め定められた本来のネットワーク環境からのアクセスを行う限り、本来のアクセス権が与えられることになるが、それ以外のネットワーク環境からアクセスした場合、ユーザのアクセス権は制限されることになる。上述の例の場合、人事部員であるユーザ甲は、人事部１０に設置されたクライアントコンピュータ１１～１４を用いてアクセスする限りは、人事部員に与えられる本来のアクセス権をもって各サーバコンピュータへのアクセスが可能になるが、談話室２０や社員寮３０に設置されたクライアントコンピュータを利用した場合は、本来のアクセス権を取得することはできない。したがって、§０で述べたようなセキュリティ上の問題を解決することができる。

【００８６】

この第２の実施形態においても、環境情報の照合処理や、照合結果に応じたアクセス権の設定処理を行うために、クライアントコンピュータ内にそれなりの構成要素を用意しておく必要がある。図６は、この第２の実施形態を行うためのクライアントコンピュータ１１の構成を示すブロック図である。図示のとおり、クライアントコンピュータ１１には、サーバアクセス手段１１Ａ，アクセス権設定手段１１Ｂ，環境照合手段１１Ｈ，インターフェイス手段１１Ｄが設けられている。もちろん、クライアントコンピュータ１１には、この他にも、クライアントコンピュータとしての機能を果たすための種々の構成要素（たとえば、ＯＳプログラムやアプリケーションプログラムを実行するためのＣＰＵ、メモリ、ハードディスクや、入出力装置など）が備わっているが、ここでは説明は省略する。

【００８７】

このクライアントコンピュータ１１は、特定のネットワーク環境下でネットワーク網１００に接続されており、当該特定のネットワーク環境は、所定の環境情報ＥＮＶ（１１）によって示すことができる。環境情報ＥＮＶ（１１）としては、クライアントコンピュータ１１に設定されたＩＰアドレス、デフォルトゲートウエイアドレス、プロキシサーバアドレスなどを用いることができる点は、既に述べたとおりである。

【００８８】

インターフェイス手段１１Ｄは、図３に示す実施形態の場合と同様に、携帯可能情報記録媒体Ｒ１１を接続するための構成要素であり、ＩＣカード用のリーダライタ装置によって構成されている。ユーザは、このクライアントコンピュータ１１に対する利用開始手続を行う際に、ＩＣカードとしての携帯可能情報記録媒体Ｒ１１を、リーダライタ装置としてのインターフェイス手段１１Ｄに装填することにより、両者を接続状態にすることができる。また、利用を終了する際には、このＩＣカードを、リーダライタ装置から引き抜くことにより、両者を分離することができる。

【００８９】

環境照合手段１１Ｈは、現在接続中の携帯可能情報記録媒体に記録されている環境情報とクライアントコンピュータ１１の現在のネットワーク環境を示す環境情報とを照合する機能を有する構成要素であり、アクセス権設定手段１１Ｂは、この照合結果に基づいて所定のアクセス権を設定する機能を有する構成要素である。アクセス権設定手段１１Ｂは、照合結果が一致した場合には第１のアクセス権を設定し、照合結果が一致しなかった場合にはこの第１のアクセス権よりも制限事項の多い第２のアクセス権を設定することになる。サーバアクセス手段１１Ａは、設定されたアクセス権の範囲内で、サーバコンピュータ１１０，１２０に対するアクセスを行う構成要素である。

【００９０】

図６に示す例の場合、ユーザ甲が自己の社員証である携帯可能情報記録媒体Ｒ１１を用いて、クライアントコンピュータ１１への利用開始手続を行っているので、環境照合手段１１Ｈによる照合結果は一致する。すなわち、環境照合手段１１Ｈは、インターフェイス手段１１Ｄを介して読み出した携帯可能情報記録媒体Ｒ１１内の環境情報ＥＮＶ（１１）と、クライアントコンピュータ１１の現時点のネットワーク環境を示す環境情報ＥＮＶ（１１）とを比較照合する処理を行うことになるので、この例の場合は、両者が一致する結果が得られ、アクセス権設定手段１１Ｂは、第１のアクセス権を設定する。

【００９１】

もし、談話室２０に設置されたクライアントコンピュータ２１に対して、同様の利用開始手続を行ったとすると、携帯可能情報記録媒体Ｒ１１内の環境情報ＥＮＶ（１１）と、クライアントコンピュータ２１のネットワーク環境を示す環境情報ＥＮＶ（２１）とは一致しないので、クライアントコンピュータ２１内の環境照合手段２１Ｈは不一致の結果を示し、アクセス権設定手段２１Ｂは、第２のアクセス権を設定することになる。第１のアクセス権によるアクセスと、第２のアクセス権によるアクセスとの相違は、既に、§１で述べたとおりである。

【００９２】

図７は、この第２の実施形態において、携帯可能情報処理装置側で照合処理およびアクセス権の設定処理を実行する変形例の構成を示すブロック図である。図示のとおり、クライアントコンピュータ１１には、現在接続中の携帯可能情報処理装置から伝達されてきたアクセス権の範囲内でサーバコンピュータに対するアクセスを行うサーバアクセス手段１１Ａと、携帯可能情報処理装置を接続するためのインターフェイス手段１１Ｄと、が備わっているものの、環境照合手段およびアクセス権設定手段は備わっていない。

【００９３】

一方、携帯可能情報処理装置Ｐ１１は、情報処理機能をもったＩＣカードであり、図示のとおり、環境照合手段１１Ｉ，アクセス権設定手段１１Ｆ，アクセス権伝達手段１１Ｇを備えている。環境照合手段１１Ｉは、現在接続中のクライアントコンピュータのネットワーク環境を示す環境情報と自分自身に記録されている環境情報とを照合する構成要素であり、アクセス権設定手段１１Ｆは、この照合結果に基づいて所定のアクセス権を設定する構成要素であり、アクセス権伝達手段１１Ｇは、設定されたアクセス権を現在接続中のクライアントコンピュータに伝達する構成要素である。

【００９４】

図示のように、ユーザ甲が自己の社員証である携帯可能情報処理装置Ｐ１１（情報処理機能をもったＩＣカード）を用いて、クライアントコンピュータ１１への利用開始手続を行うと、環境照合手段１１Ｉは、インターフェイス手段１１Ｄを介して読み出したクライアントコンピュータ１１のネットワーク環境を示す環境情報ＥＮＶ（１１）と、携帯可能情報処理装置Ｐ１１内に記録されていた環境情報ＥＮＶ（１１）とを比較照合する処理を行うことになる。この例の場合は、両者が一致する結果が得られるので、アクセス権設定手段１１Ｆは、第１のアクセス権を設定し、設定したアクセス権は、インターフェイス手段１１Ｄを介して、サーバアクセス手段１１Ａへと伝えられる。その結果、サーバアクセス手段１１Ａは、第１のアクセス権に基づいてサーバコンピュータへのアクセスを行うことになる。

【００９５】
もちろん、談話室２０に設置されたクライアントコンピュータ２１に対して、同様の利用開始手続を行ったとすると、携帯可能情報処理装置Ｐ１１内の環境情報ＥＮＶ（１１）と、クライアントコンピュータ２１のネットワーク環境を示す環境情報ＥＮＶ（２１）とは一致しないので、環境照合手段１１Ｉでは、不一致の照合結果が得られることになり、アクセス権設定手段１１Ｆは、第２のアクセス権を設定する。その結果、サーバアクセス手段１１Ａは、第２のアクセス権に基づいてサーバコンピュータへのアクセスを行うことになる。

【００９６】
＜＜＜　§３．本発明の第３の実施形態　＞＞＞
ここで述べる第３の実施形態は、§１で述べた第１の実施形態と§２で述べた第２の実施形態との組み合わせに相当するものである。すなわち、第１の実施形態の特徴は、個々のユーザに対して、それぞれ本来利用すべき特定のクライアントコンピュータを設定しておき、当該クライアントコンピュータからのアクセスか否かによって、アクセス権の設定を変えることにあり、第２の実施形態の特徴は、個々のユーザに対して、それぞれ本来利用すべき特定のネットワーク環境を設定しておき、当該ネットワーク環境からのアクセスか否かによって、アクセス権の設定を変えることにある。ここで述べる第３の実施形態の特徴は、個々のユーザに対して、それぞれ本来利用すべき特定のクライアントコンピュータと、本来利用すべき特定のネットワーク環境とを設定しておき、当該クライアントコンピュータからのアクセスか否かという点と、当該ネットワーク環境からのアクセスか否かという点とを考慮して、アクセス権の設定を変えることにある。

【００９７】
したがって、この第３の実施形態では、個々のユーザに対して発行した携帯可能情報記録媒体に特定の識別コードと、特定のネットワーク環境を示す環境情報と、を記録しておくことになる。ユーザが、クライアントコンピュータに対して利用開始手続を行うと、当該クライアントコンピュータに記録されている識別コードと携帯可能情報記録媒体に記録されている識別コードとの照合処理と、当該クライアントコンピュータの現在のネットワーク環境と携帯可能情報記録媒体に記録されている環境情報によって示されるネットワーク環境との照合処理が行われ、これらの照合結果に基づいて所定のアクセス権が設定されることになる。

【００９８】
図８は、本発明の第３の実施形態を説明するためのブロック図であり、図１に示すコンピュータシステムの一部を示すものである。ここでも、３人のユーザ甲，乙，丙に対して、それぞれ携帯可能情報記録媒体Ｒ１１，Ｒ１２，Ｒ２１が発行された例が示されている。個々の携帯可能情報記録媒体Ｒ１１，Ｒ１２，Ｒ２１には、所定の識別コードとともに、所定の環境情報が記録されている。たとえば、ユーザ甲に発行された携帯可能情報記録媒体Ｒ１１（ユーザ甲の社員証として発行されたＩＣカード）には、ユーザ甲が本来利用すべきクライアントコンピュータ１１の識別コードＩＤ（１１）と、ユーザ甲が本来利用すべきネットワーク環境を示す環境情報ＥＮＶ（１１）とが記録されている。同様に、ユーザ乙に発行された携帯可能情報記録媒体Ｒ１２には、ユーザ乙が本来利用すべきクライアントコンピュータ１２の識別コードＩＤ（１２）と、ユーザ乙が本来利用すべきネットワーク環境を示す環境情報ＥＮＶ（１２）とが記録されており、ユーザ丙に発行された携帯可能情報記録媒体Ｒ２１には、ユーザ丙が本来利用すべきクライアントコンピュータ２１の識別コードＩＤ（２１）と、ユーザ丙が本来利用すべきネットワーク環境を示す環境情報ＥＮＶ（２１）とが記録されている。

【００９９】
この図８に示す例において、たとえばユーザ甲が、自己の社員証として発行された携帯可能情報記録媒体Ｒ１１を、人事部１０のクライアントコンピュータ１１に接続して利用開始手続を行った場合、クライアントコンピュータ１１内の識別コードＩＤ（１１）と、携帯可能情報記録媒体Ｒ１１に記録されている識別コード（１１）との照合作業が行われ

るとともに、クライアントコンピュータ１１のネットワーク環境を示す環境情報ＥＮＶ（１１）と携帯可能情報記録媒体Ｒ１１に記録されている環境情報ＥＮＶ（１１）との照合作業が行われる。そして、これらの照合結果に基づいてアクセス権が設定される。この例の場合、２つの照合結果はいずれも一致することになる。

【０１００】

もし、ユーザ甲が、クライアントコンピュータ１１の代わりに、クライアントコンピュータ１２に対して利用開始手続を行った場合は、クライアントコンピュータ１２内の識別コードＩＤ（１２）と、携帯可能情報記録媒体Ｒ１１に記録されている識別コード（１１）との照合作業が行われるとともに、クライアントコンピュータ１２のネットワーク環境を示す環境情報ＥＮＶ（１２）と携帯可能情報記録媒体Ｒ１１に記録されている環境情報ＥＮＶ（１１）との照合作業が行われる。この場合、識別コードについての照合作業では、ＩＤ（１１）≠ＩＤ（１２）と不一致になるが、ネットワーク環境についての照合作業では、ＥＮＶ（１１）＝ＥＮＶ（１２）と一致する。

【０１０１】

一方、ユーザ甲が、談話室２０に設置されたクライアントコンピュータ２１を利用したアクセスを行った場合は、識別コードについての照合作業では、ＩＤ（１１）≠ＩＤ（２１）と不一致になり、ネットワーク環境についての照合作業でも、ＥＮＶ（１１）≠ＥＮＶ（２１）と不一致になる。また、ユーザ甲が、人事部１０に設置されているクライアントコンピュータ１１を、談話室２０へ移動し、談話室２０のＬＡＮに接続してアクセスを行うようなことをすると、識別コードについての照合作業では、ＩＤ（１１）＝ＩＤ（１１）と一致するが、ネットワーク環境についての照合作業では、ＥＮＶ（１１）≠ＥＮＶ（２１）と不一致になる。

【０１０２】

このように、識別コードの照合作業とネットワーク環境の照合作業とを組み合わせると、合計４とおりの照合結果が得られることになり、４通りのバリエーションをもったアクセス権の設定が可能になる。

【０１０３】

図９は、この第３の実施形態を行うためのクライアントコンピュータ１１の構成を示すブロック図であり、いわば図３の構成と図６の構成とを合成したものに相当する。個々の構成要素の機能は、それぞれ§１および§２で述べたとおりであるので、ここでは各構成要素の機能の説明は省略する。図示のとおり、携帯可能情報記録媒体Ｒ１１には、識別コードＩＤ（１１）と環境情報ＥＮＶ（１１）との双方が記録されている。また、クライアントコンピュータ１１側には、識別コードの照合作業を行う識別コード照合手段１１Ｃと、ネットワーク環境の照合を行う環境照合手段１１Ｈとの双方が設けられており、アクセス権設定手段１１Ｂは、この２つの照合結果に基づいて、所定のアクセス権の設定を行うことになる。

【０１０４】

図１０は、この第３の実施形態において、携帯可能情報処理装置側で照合処理およびアクセス権の設定処理を実行する変形例の構成を示すブロック図である。このブロック図は、いわば図４の構成と図７の構成とを合成したものに相当する。ここでも、個々の構成要素の機能は、それぞれ§１および§２で述べたとおりであるので、各構成要素の機能の説明は省略する。図示のとおり、携帯可能情報処理装置Ｐ１１には、識別コードＩＤ（１１）と環境情報ＥＮＶ（１１）との双方が記録されており、また、識別コードの照合作業を行う識別コード照合手段１１Ｅと、ネットワーク環境の照合を行う環境照合手段１１Ｉとの双方が設けられている。アクセス権設定手段１１Ｆは、この２つの照合結果に基づいて、所定のアクセス権の設定を行うことになる。

【０１０５】

上述したように、この第３の実施形態では、識別コードの照合作業とネットワーク環境の照合作業とを組み合わせることにより、合計４とおりの照合結果が得られるので、４通りのバリエーションをもったアクセス権の設定が可能になるが、実際には、３通りのアク

セス権設定を行えば十分である。ここでは、多くの企業で利用されているコンピュータシステムに適用することが可能な２つの実用的なアクセス権の設定アルゴリズムを例示しておくことにする。

【０１０６】

まず、第１のアルゴリズムは、識別コードの照合結果が一致した場合には、ネットワーク環境の照合結果にかかわらず第１のアクセス権を設定し、識別コードの照合結果は一致しないがネットワーク環境の照合結果が一致した場合には、第１のアクセス権よりも制限事項の多い第２のアクセス権を設定し、いずれの照合結果も一致しなかった場合には、第２のアクセス権よりも更に制限事項の多い第３のアクセス権を設定する方法である。この方法によれば、実際のコンピュータシステムの運用に即したアクセス権管理が可能になる。

【０１０７】

図１１は、このような方針に基づくアクセス権の設定方法を示す流れ図である。まず、ステップＳ１において、ユーザが所定のクライアントコンピュータへの利用開始手続を行ったとすると、ステップＳ２において、識別コードの照合作業が行われる。ここで、識別コードが一致した場合には、ステップＳ３を経てステップＳ６へと分岐し、制限事項の少ない第１のアクセス権が設定される。この場合、ネットワーク環境の照合作業は行う必要はない。一方、識別コードが不一致であった場合には、ステップＳ３を経てステップＳ４へと進み、ここでネットワーク環境の照合作業が行われる。そして、ネットワーク環境が一致した場合には、ステップＳ５を経てステップＳ７へと分岐し、制限事項が中ぐらいの第２のアクセス権が設定される。一方、ネットワーク環境も不一致であった場合には、ステップＳ５を経てステップＳ８へと分岐し、制限事項の多い第３のアクセス権が設定される。

【０１０８】

結局、この図１１に示すアルゴリズムに基づいてアクセス権の設定を行えば、ユーザが、自分自身に支給された本来のクライアントコンピュータ自体を利用している限り、それをどのようなネットワーク環境で利用していたとしても、最もレベルの高い第１のアクセス権（当該ユーザに本来与えられるべきアクセス権）が与えられることになる。一方、ユーザがそれ以外のクライアントコンピュータを利用してアクセスした場合には、本来のネットワーク環境からのアクセスである場合には、中レベルの第２のアクセス権が与えられることになり、それ以外のネットワーク環境からのアクセスである場合には、最もレベルの低い第３のアクセス権が与えられることになる。

【０１０９】

一方、第２のアルゴリズムは、識別コード照合手段による照合結果と環境照合手段による照合結果との双方が一致した場合には第１のアクセス権を設定し、識別コード照合手段による照合結果は一致したが環境照合手段による照合結果は一致しない場合には第１のアクセス権よりも制限事項の多い第２のアクセス権を設定し、いずれの照合結果も一致しなかった場合には第２のアクセス権よりも更に制限事項の多い第３のアクセス権を設定する方法である。この方法でも、実際のコンピュータシステムの運用に即したアクセス権管理が可能になる。

【０１１０】

図１２は、このような方針に基づくアクセス権の設定方法を示す流れ図である。まず、ステップＳ１において、ユーザが所定のクライアントコンピュータへの利用開始手続を行ったとすると、ステップＳ２において、識別コードの照合作業が行われる。ここで、識別コードが一致した場合には、ステップＳ３を経てステップＳ４へと分岐し、ネットワーク環境の照合作業が行われる。そして、ネットワーク環境も一致した場合には、ステップＳ５を経てステップＳ６へと分岐し、制限事項の少ない第１のアクセス権が設定される。もし、ネットワーク環境が不一致であった場合には、ステップＳ５を経てステップＳ７へと分岐し、制限事項が中ぐらいの第２のアクセス権が設定される。一方、識別コードが不一致であった場合には、ステップＳ３からステップＳ８へと分岐し、制限事項の多い第３の

アクセス権が設定される。この場合、ネットワーク環境の照合作業は行う必要はない。

【０１１１】

結局、この図１２に示すアルゴリズムに基づいてアクセス権の設定を行えば、ユーザが、自分自身に支給された本来のクライアントコンピュータ自体を、本来のネットワーク環境で利用している限り、最もレベルの高い第１のアクセス権（当該ユーザに本来与えられるべきアクセス権）が与えられることになる。また、ユーザが、自分自身に支給された本来のクライアントコンピュータ自体を利用しているものの、本来のネットワーク環境ではない異なるネットワーク環境から利用している場合には、中レベルの第２のアクセス権が与えられることになる。一方、ユーザが、自分自身に支給された本来のクライアントコンピュータではない他のクライアントコンピュータから利用している場合は、そのネットワーク環境にかかわらず、最もレベルの低い第３のアクセス権が与えられることになる。

【０１１２】

以上、この第３の実施形態に利用可能なアクセス権の設定アルゴリズムを２通りの事例について説明したが、もちろん、本発明におけるアクセス権の設定は、個々のコンピュータシステムに適合するように自由に行うことができ、上述した例に限定されるものではない。たとえば、４通りの照合結果に基づいて、４通りのアクセス権を設定するようにしてもかまわない。

【０１１３】

＜＜＜　§４．いくつかの変形例　＞＞＞

以上、本発明を３つの基本的な実施形態に基づいて説明したが、本発明はこれらの実施形態に限定されるものではなく、この他にも種々の形態で実施可能である。ここでは、最後に、本発明を実施する上でのいくつかの変形例を述べておく。

【０１１４】

(1)　本発明の特徴は、識別コードの照合結果もしくはネットワーク環境の照合結果に基づいて所定のアクセス権の設定を行う点にあるが、実用上は、もちろん、従来から行われているように、アカウントおよびパスワードによりユーザを認証し、予めユーザごとに設定された所定のアクセス権を与える手法と組み合わせて利用することができる。

【０１１５】

(2)　上述の実施形態では、携帯可能情報記録媒体内に記録する識別コードや環境情報を単一のものとする例を示したが、複数の識別コードや複数のネットワーク環境を記録しておき、それぞれについて照合を行うようにしてもかまわない。この場合、どの識別コードが一致したか、あるいは、どのネットワーク環境が一致したか、によって、それぞれ異なるアクセス権を設定することもできる。たとえば、ユーザ甲に発行した携帯可能情報記録媒体Ｒ１１内に、２通りの識別コードＩＤ（１１－１）およびＩＤ（１１－２）を記録しておき、識別コードＩＤ（１１－１）が一致した場合には第１のアクセス権、識別コードＩＤ（１１－２）が一致した場合には第２のアクセス権、をそれぞれ設定するようにすることも可能である。

【０１１６】

(3)　上述の実施形態では、識別コードや環境情報が一致する例として、コードやアドレスを示す文字列が完全に一致する例を述べたが、本発明における照合一致とは、必ずしも文字列等が１対１に完全に対応する場合を意味するものではなく、クライアントコンピュータ側の情報と、携帯可能情報記録媒体側の情報とが、何らかの形で対応していることを意味するものである。たとえば、クライアントコンピュータ側の情報がＡであり、携帯可能情報記録媒体側の情報がＢであったとしても、情報Ａに特定の演算処理を施すことにより情報Ｂが一義的に得られる関係になっているのであれば、当該特定の演算処理の実施により、情報Ａと情報Ｂとが対応していることを確認することができるので、照合一致と判断することができる。

【０１１７】

(4)　本発明におけるアクセス権とは、ファイルに対する読出し／書き込みを許可する権利のみならず、たとえば、ファイルの内容をプリントアウトする許可を与える権利など

、様々な処理についての権利を含むものである。

【０１１８】

(5)　本発明にいう「サーバコンピュータ」とは、データやサービスを提供する側のコンピュータを広く意味し、「クライアントコンピュータ」とは、データやサービスの提供を受ける側のコンピュータを広く意味するものである。したがって、たとえば、図１に示す構成において、クライアントコンピュータ１１が、クライアントコンピュータ１４内に格納されているデータをネットワークで転送するような処理を実行した場合には、このような処理に関しては、クライアントコンピュータ１４は「サーバコンピュータ」として機能することになる。

【０１１９】

(6)　図３，図４，図６，図７，図９，図１０では、クライアントコンピュータや携帯可能情報処理装置の個々の構成要素を、それぞれブロックとして示したが、これらの各ブロックは、実際には、コンピュータやＩＣカードに組み込まれたプログラムによって実現される構成要素である。もちろん、当該プログラムは、ＣＤ－ＲＯＭなどのコンピュータ読み取り可能な記録媒体に記録して配付することも可能である。

【図面の簡単な説明】

【０１２０】

【図１】ネットワーク網にサーバコンピュータとクライアントコンピュータとを接続して構成される一般的なコンピュータシステムを示すブロック図である。

【図２】本発明の第１の実施形態を説明するためのブロック図であり、図１に示すコンピュータシステムの一部を示すものである。

【図３】図２に示す第１の実施形態を行うためのクライアントコンピュータの構成を示すブロック図である。

【図４】図２に示す第１の実施形態において、携帯可能情報処理装置側で照合処理およびアクセス権の設定処理を実行する変形例の構成を示すブロック図である。

【図５】本発明の第２の実施形態を説明するためのブロック図であり、図１に示すコンピュータシステムの一部を示すものである。

【図６】図５に示す第２の実施形態を行うためのクライアントコンピュータの構成を示すブロック図である。

【図７】図５に示す第２の実施形態において、携帯可能情報処理装置側で照合処理およびアクセス権の設定処理を実行する変形例の構成を示すブロック図である。

【図８】本発明の第３の実施形態を説明するためのブロック図であり、図１に示すコンピュータシステムの一部を示すものである。

【図９】図８に示す第３の実施形態を行うためのクライアントコンピュータの構成を示すブロック図である。

【図１０】図８に示す３の実施形態において、携帯可能情報処理装置側で照合処理およびアクセス権の設定処理を実行する変形例の構成を示すブロック図である。

【図１１】本発明の第３の実施形態におけるアクセス権の設定方法の一例を示す流れ図である。

【図１２】本発明の第３の実施形態におけるアクセス権の設定方法の別な一例を示す流れ図である。

【符号の説明】

【０１２１】

１０…人事部

１１～１４…人事部に設置されたクライアントコンピュータ

１１Ａ…サーバアクセス手段

１１Ｂ…アクセス権設定手段

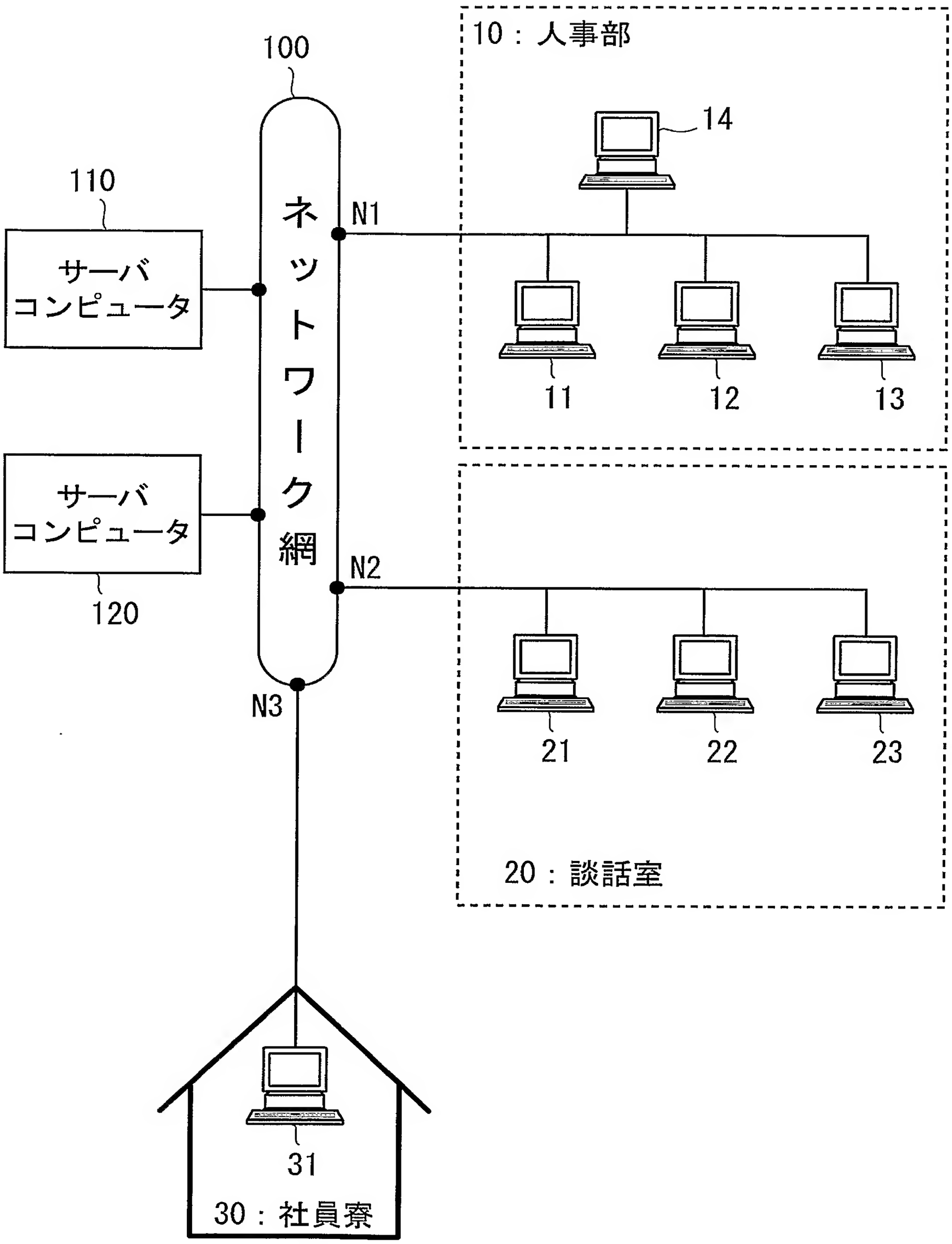
１１Ｃ…識別コード照合手段

１１Ｄ…インターフェイス手段

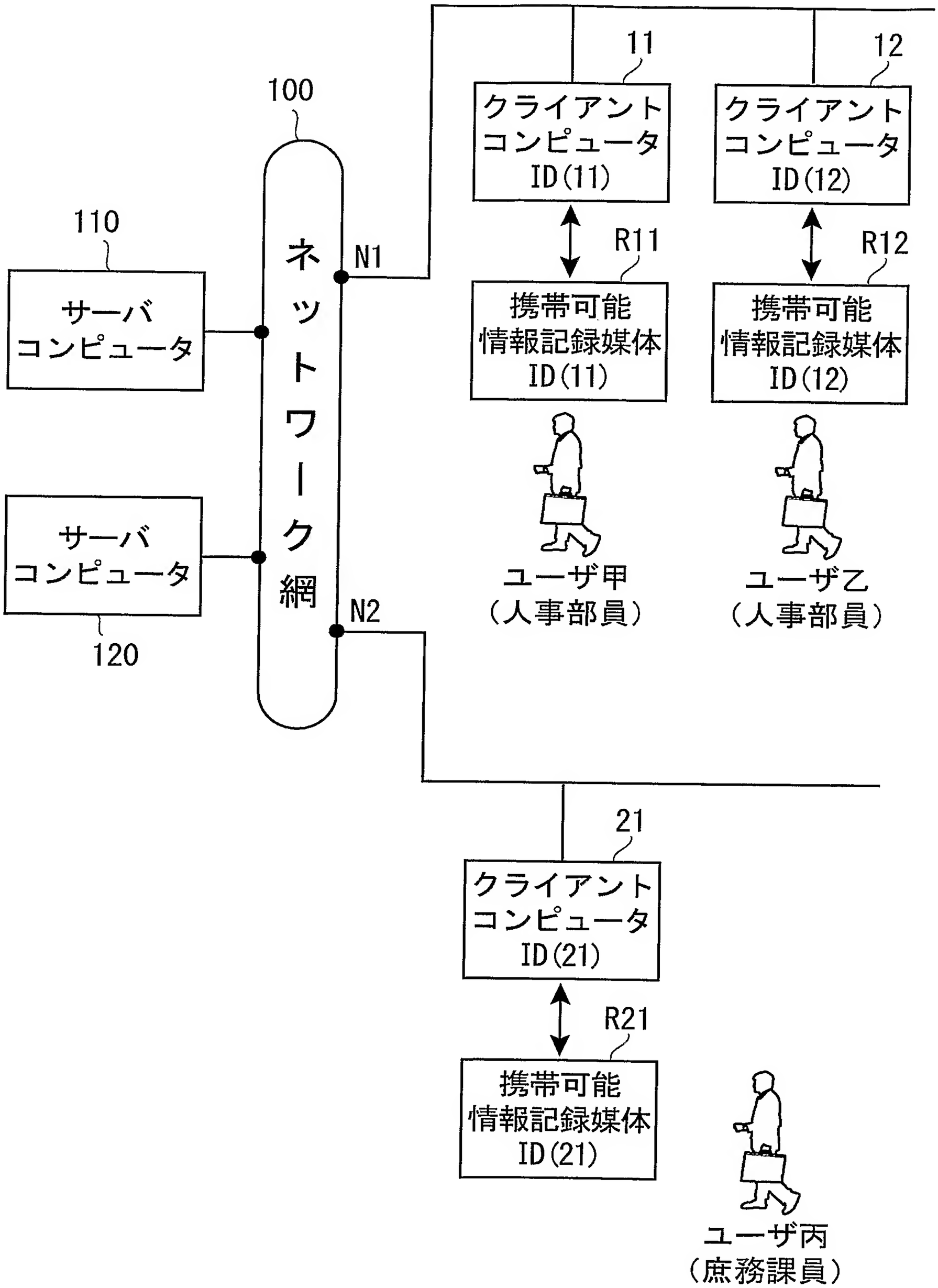
１１Ｅ…識別コード照合手段

１１Ｆ…アクセス権設定手段
１１Ｇ…アクセス権伝達手段
１１Ｈ…環境照合手段
１１Ｉ…環境照合手段
２０…談話室
２１～２３…談話室に設置されたクライアントコンピュータ
３０…社員寮
３１…社員寮に設置されたクライアントコンピュータ
１００…ネットワーク網
１１０…サーバコンピュータ
１２０…サーバコンピュータ
ＥＮＶ（１１），ＥＮＶ（１２），ＥＮＶ（２１）…ネットワーク環境を示す環境情報
ＩＤ（１１），ＩＤ（１２），ＩＤ（２１）…識別コード
Ｎ１，Ｎ２，Ｎ３…ネットワーク網の各ノード
Ｐ１１…携帯可能情報処理装置（ＩＣカード）
Ｒ１１，Ｒ１２，Ｒ２１…携帯可能情報記録媒体（ＩＣカード）
Ｓ１～Ｓ８…流れ図の各ステップ

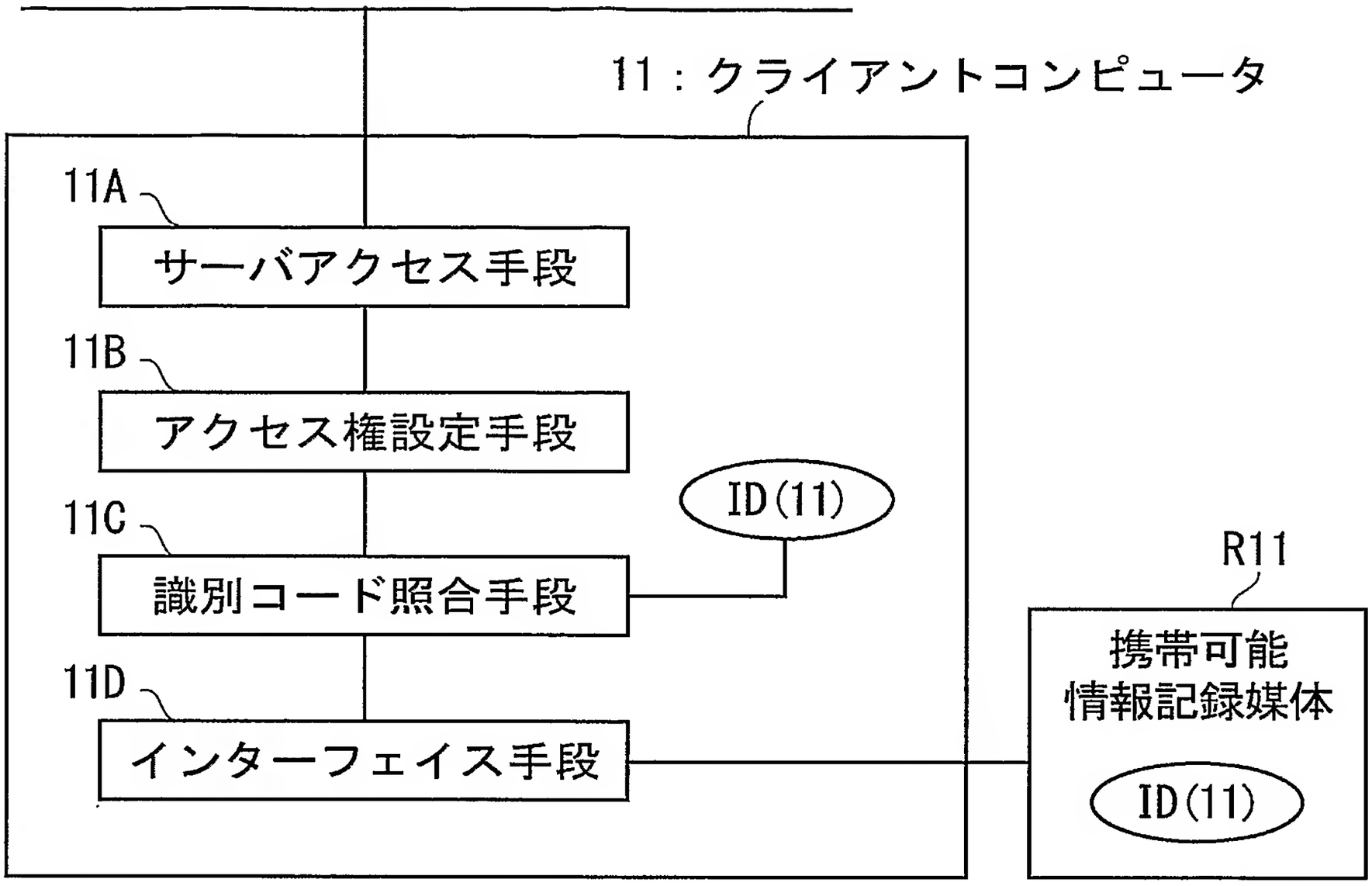
【書類名】図面
【図１】


10：人事部
100
14
110
N1
サーバ
コンピュータ
ネットワーク網
11
12
13
サーバ
コンピュータ
N2
120
N3
21
22
23
20：談話室
31
30：社員寮

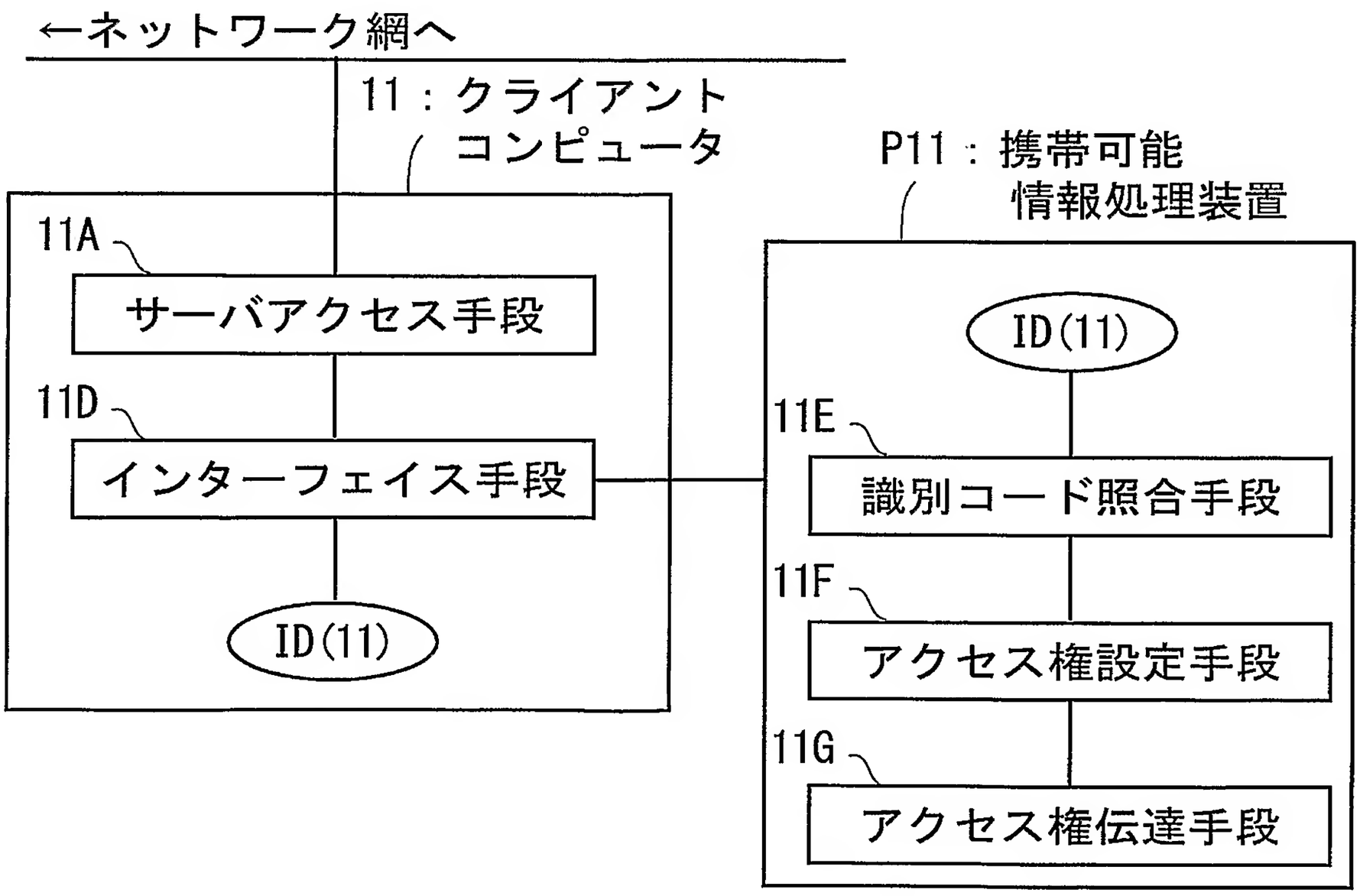
【図２】


100
ネットワーク網
110
サーバコンピュータ
120
サーバコンピュータ
N1
N2
11
クライアントコンピュータID(11)
12
クライアントコンピュータID(12)
R11
携帯可能情報記録媒体ID(11)
R12
携帯可能情報記録媒体ID(12)
ユーザ甲（人事部員）
ユーザ乙（人事部員）
21
クライアントコンピュータID(21)
R21
携帯可能情報記録媒体ID(21)
ユーザ丙（庶務課員）

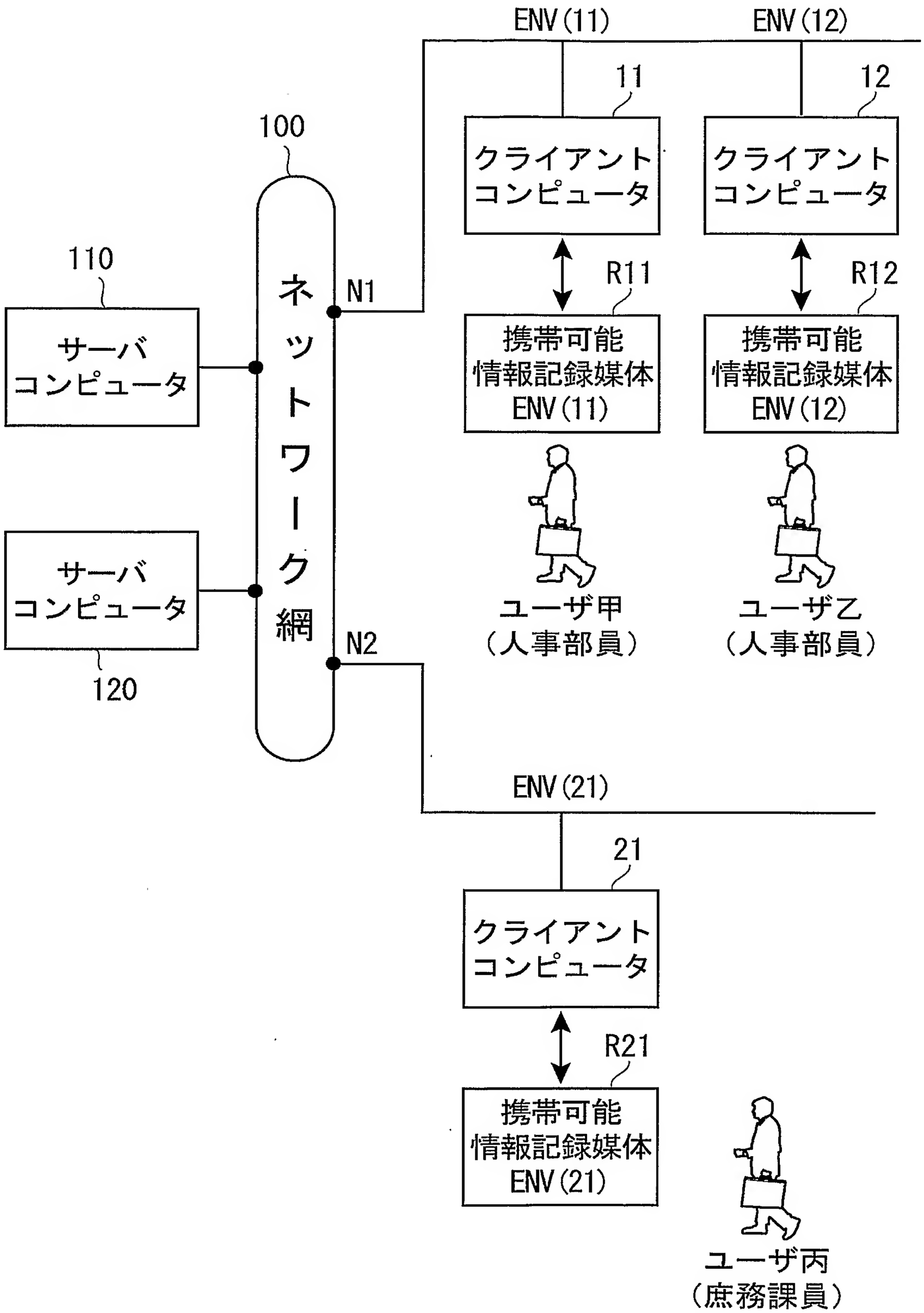
【図３】


←ネットワーク網へ
11：クライアントコンピュータ
11A
サーバアクセス手段
11B
アクセス権設定手段
ID(11)
11C
識別コード照合手段
R11
携帯可能
情報記録媒体
11D
インターフェイス手段
ID(11)

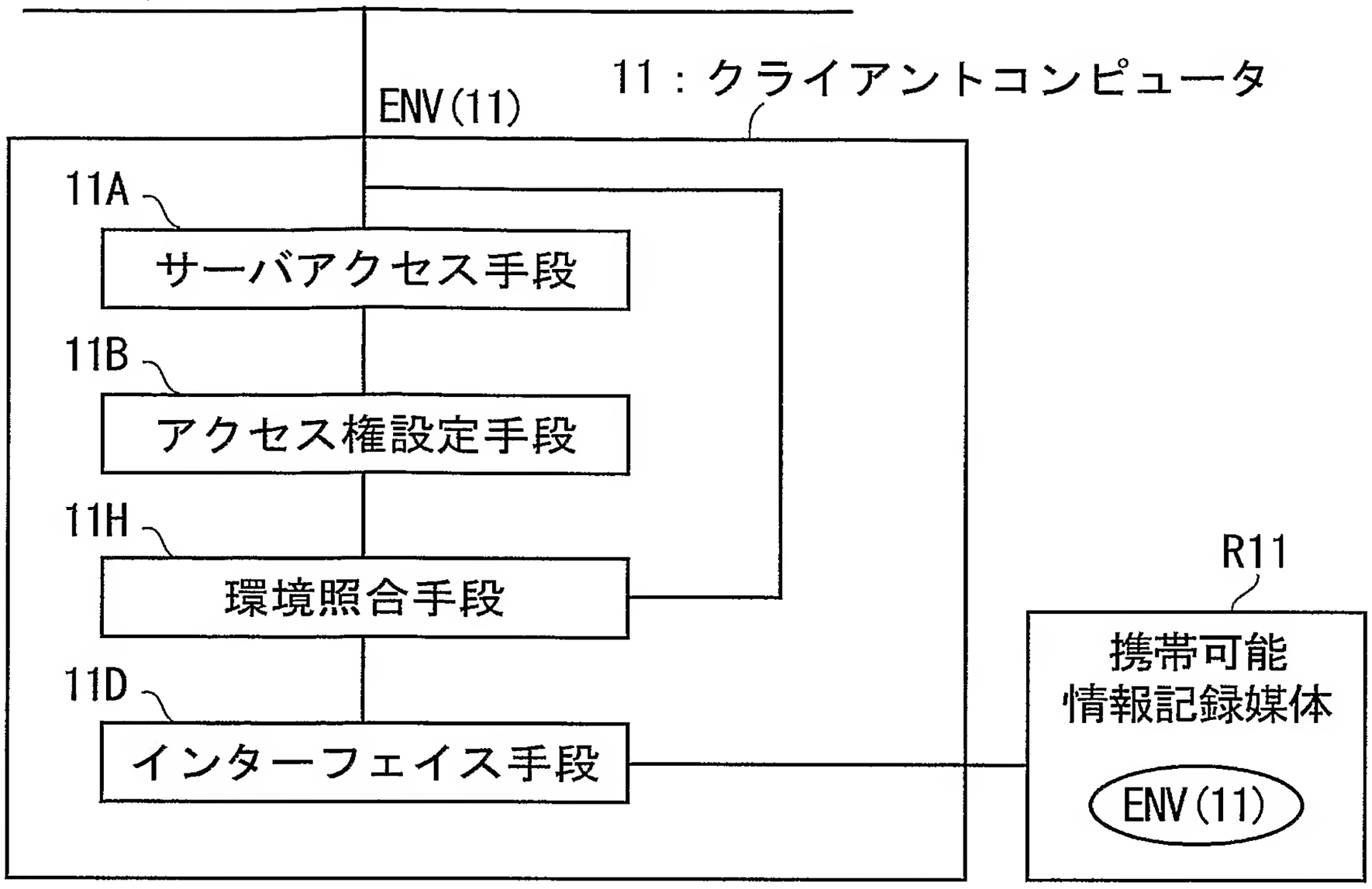
【図４】


←ネットワーク網へ
11：クライアント
コンピュータ
11A
サーバアクセス手段
11D
インターフェイス手段
ID(11)
P11：携帯可能
情報処理装置
ID(11)
11E
識別コード照合手段
11F
アクセス権設定手段
11G
アクセス権伝達手段

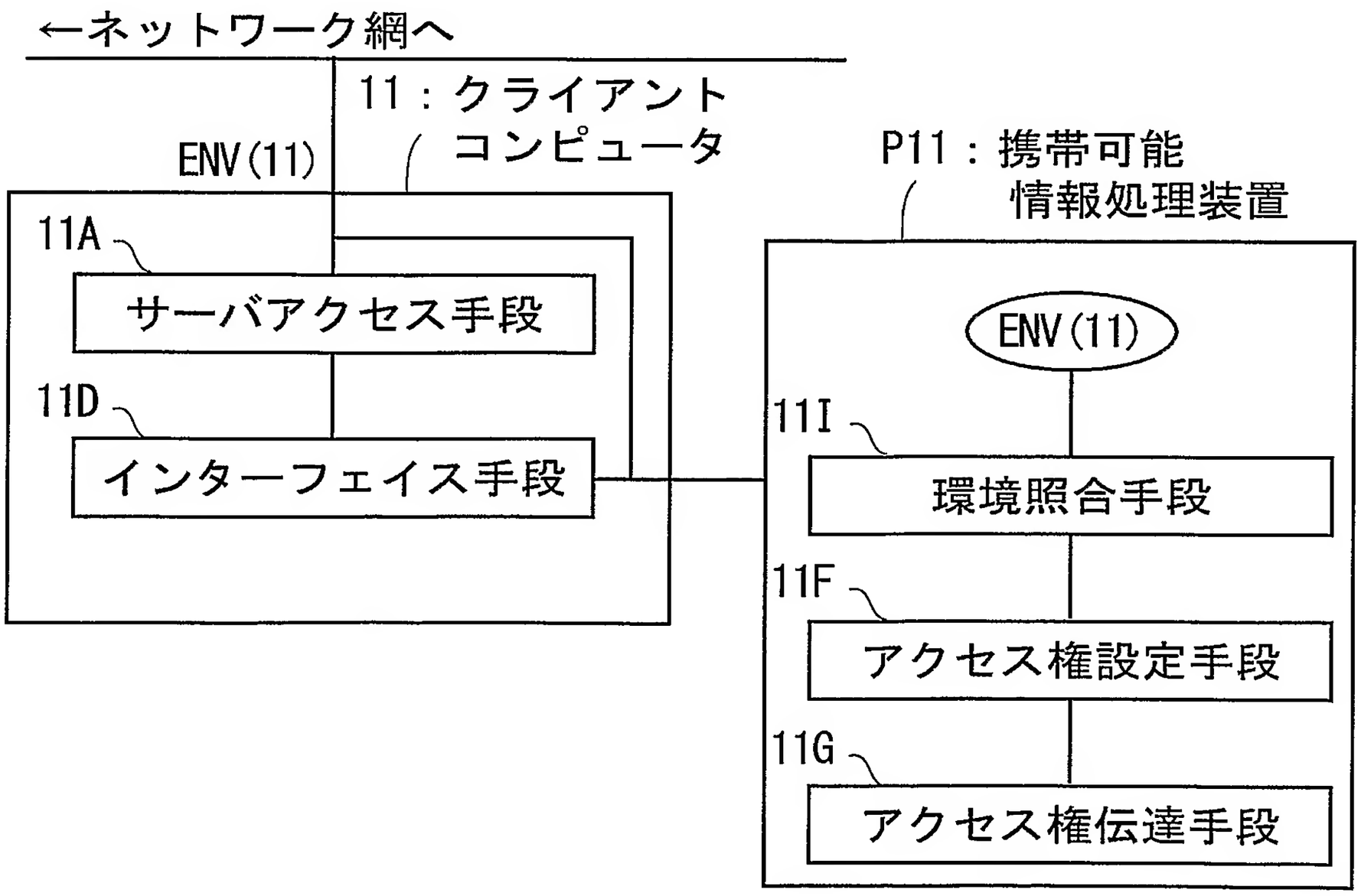
【図５】


ENV(11)
ENV(12)
11
12
100
クライアント
コンピュータ
クライアント
コンピュータ
110
R11
R12
N1
サーバ
コンピュータ
ネットワーク網
携帯可能
情報記録媒体
ENV(11)
携帯可能
情報記録媒体
ENV(12)
ユーザ甲
（人事部員）
ユーザ乙
（人事部員）
サーバ
コンピュータ
N2
120
ENV(21)
21
クライアント
コンピュータ
R21
携帯可能
情報記録媒体
ENV(21)
ユーザ丙
（庶務課員）

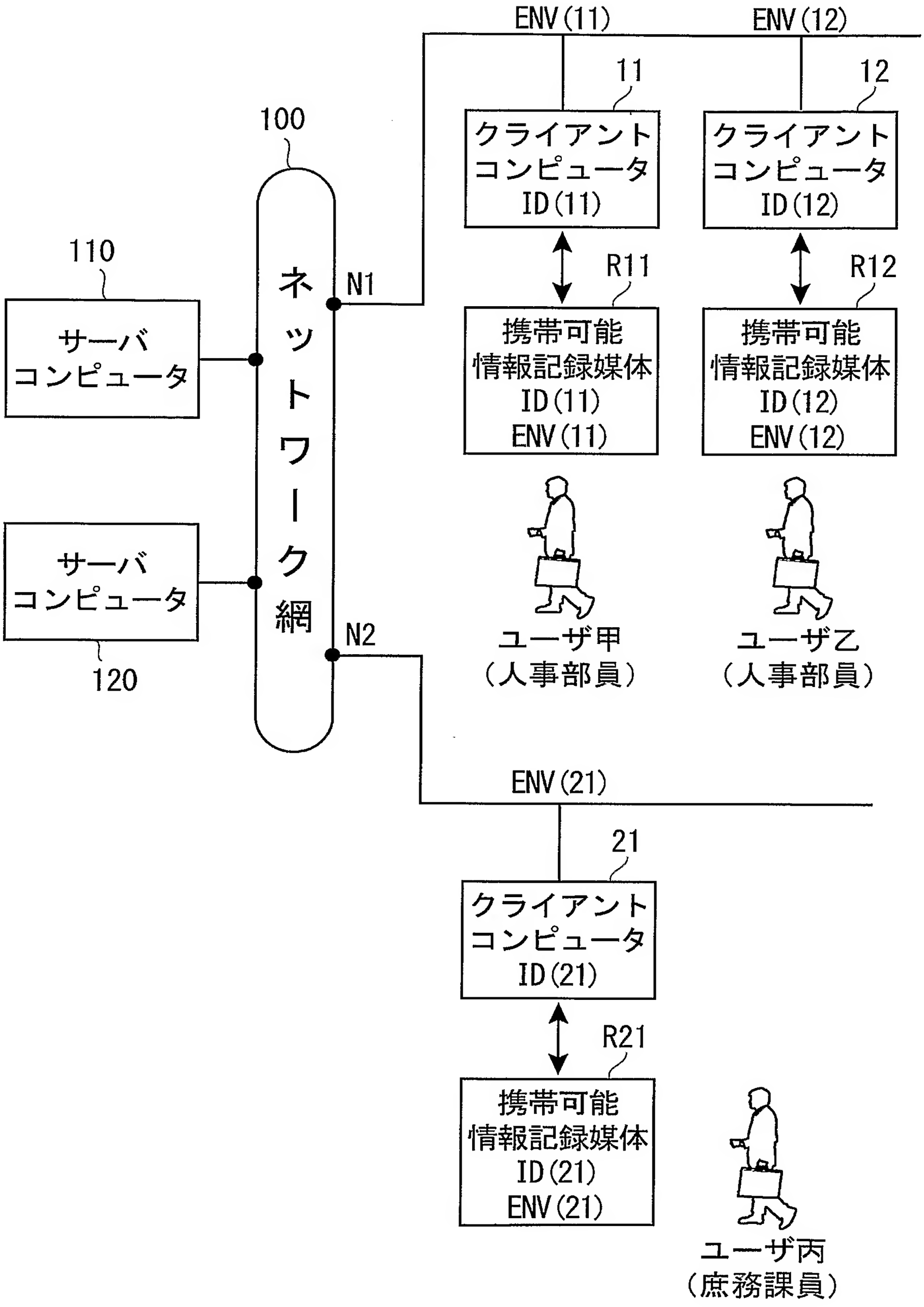
【図６】


←ネットワーク網へ
11：クライアントコンピュータ
ENV(11)
11A
サーバアクセス手段
11B
アクセス権設定手段
11H
環境照合手段
11D
インターフェイス手段
R11
携帯可能
情報記録媒体
ENV(11)

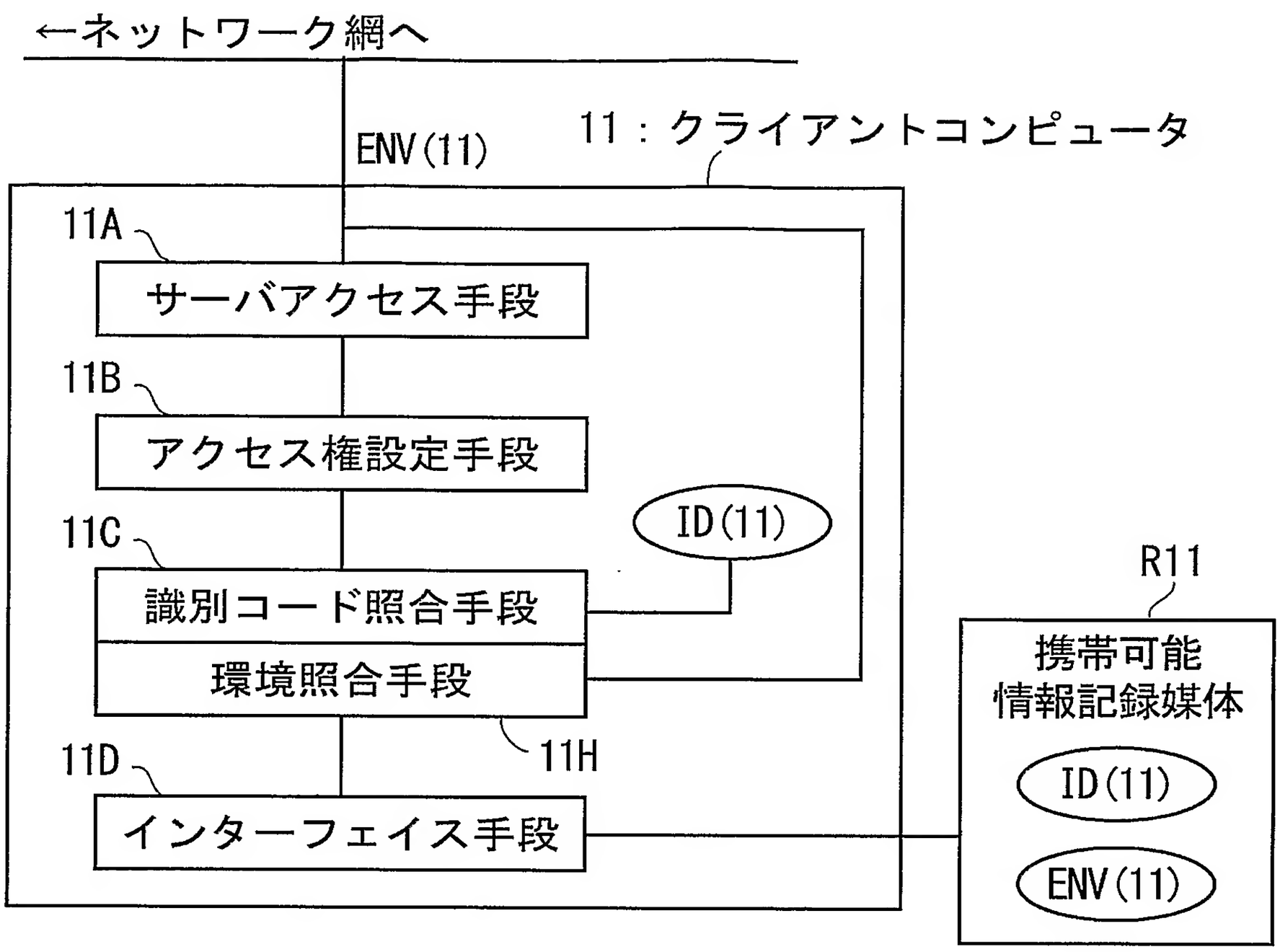
【図７】


←ネットワーク網へ
11：クライアント
コンピュータ
ENV(11)
11A
サーバアクセス手段
11D
インターフェイス手段
P11：携帯可能
情報処理装置
ENV(11)
11I
環境照合手段
11F
アクセス権設定手段
11G
アクセス権伝達手段

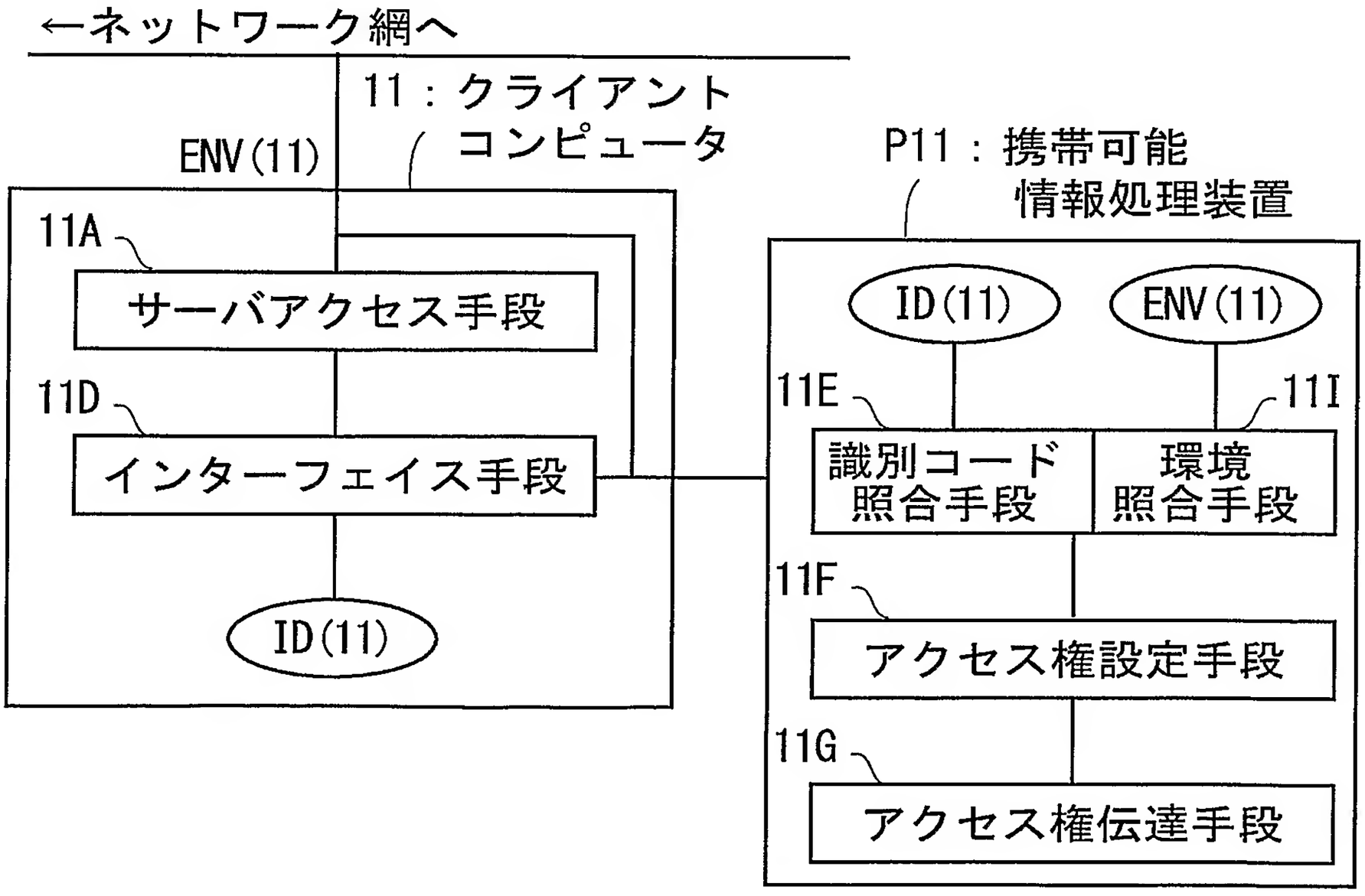
【図８】


ENV(11)
ENV(12)
11
12
100
クライアント
コンピュータ
ID(11)
クライアント
コンピュータ
ID(12)
110
R11
R12
N1
サーバ
コンピュータ
ネットワーク網
携帯可能
情報記録媒体
ID(11)
ENV(11)
携帯可能
情報記録媒体
ID(12)
ENV(12)
ユーザ甲
（人事部員）
ユーザ乙
（人事部員）
サーバ
コンピュータ
120
N2
ENV(21)
21
クライアント
コンピュータ
ID(21)
R21
携帯可能
情報記録媒体
ID(21)
ENV(21)
ユーザ丙
（庶務課員）

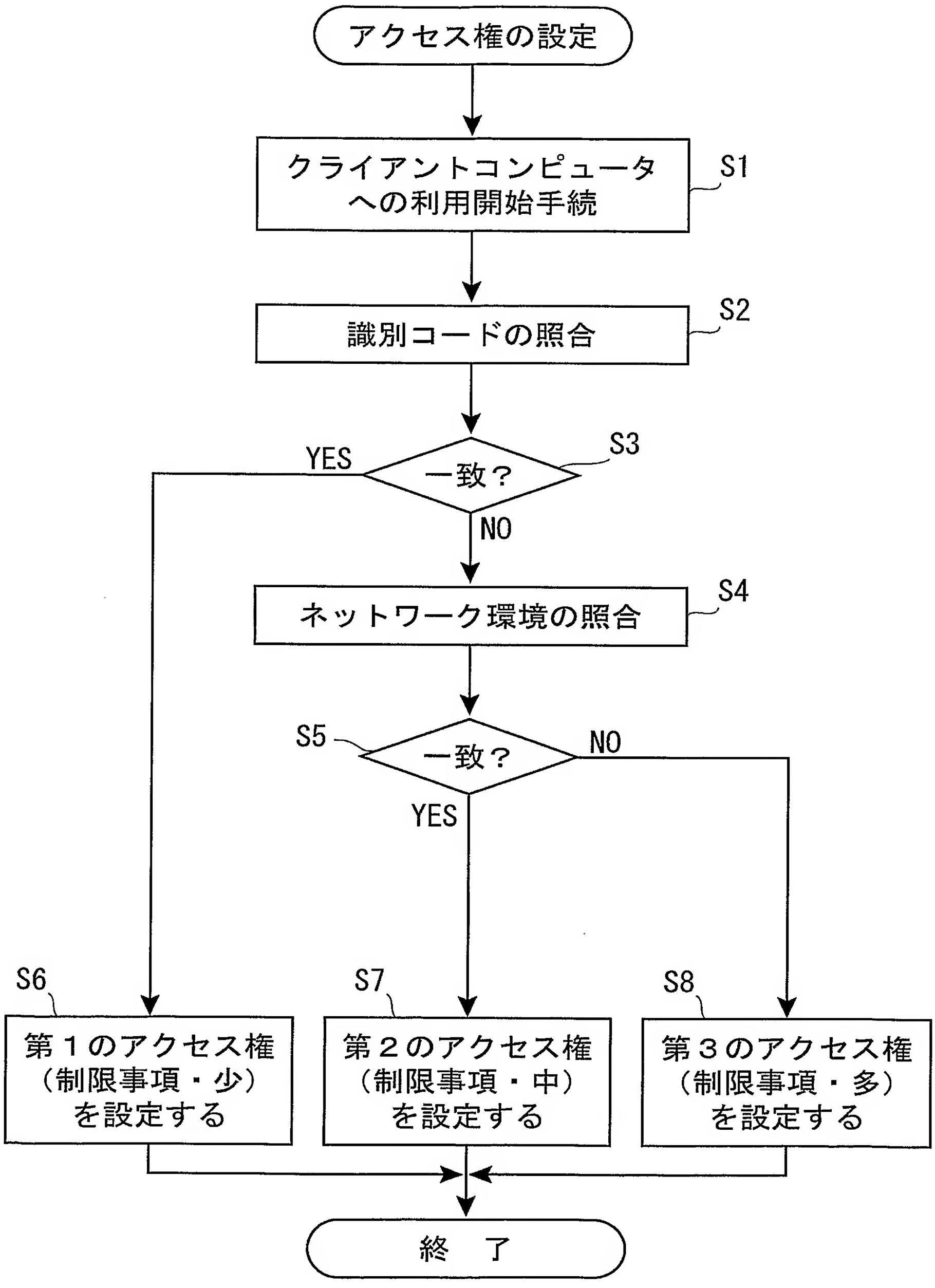
【図９】


←ネットワーク網へ
ENV(11)
11：クライアントコンピュータ
11A
サーバアクセス手段
11B
アクセス権設定手段
ID(11)
11C
識別コード照合手段
環境照合手段
11H
11D
インターフェイス手段
R11
携帯可能
情報記録媒体
ID(11)
ENV(11)

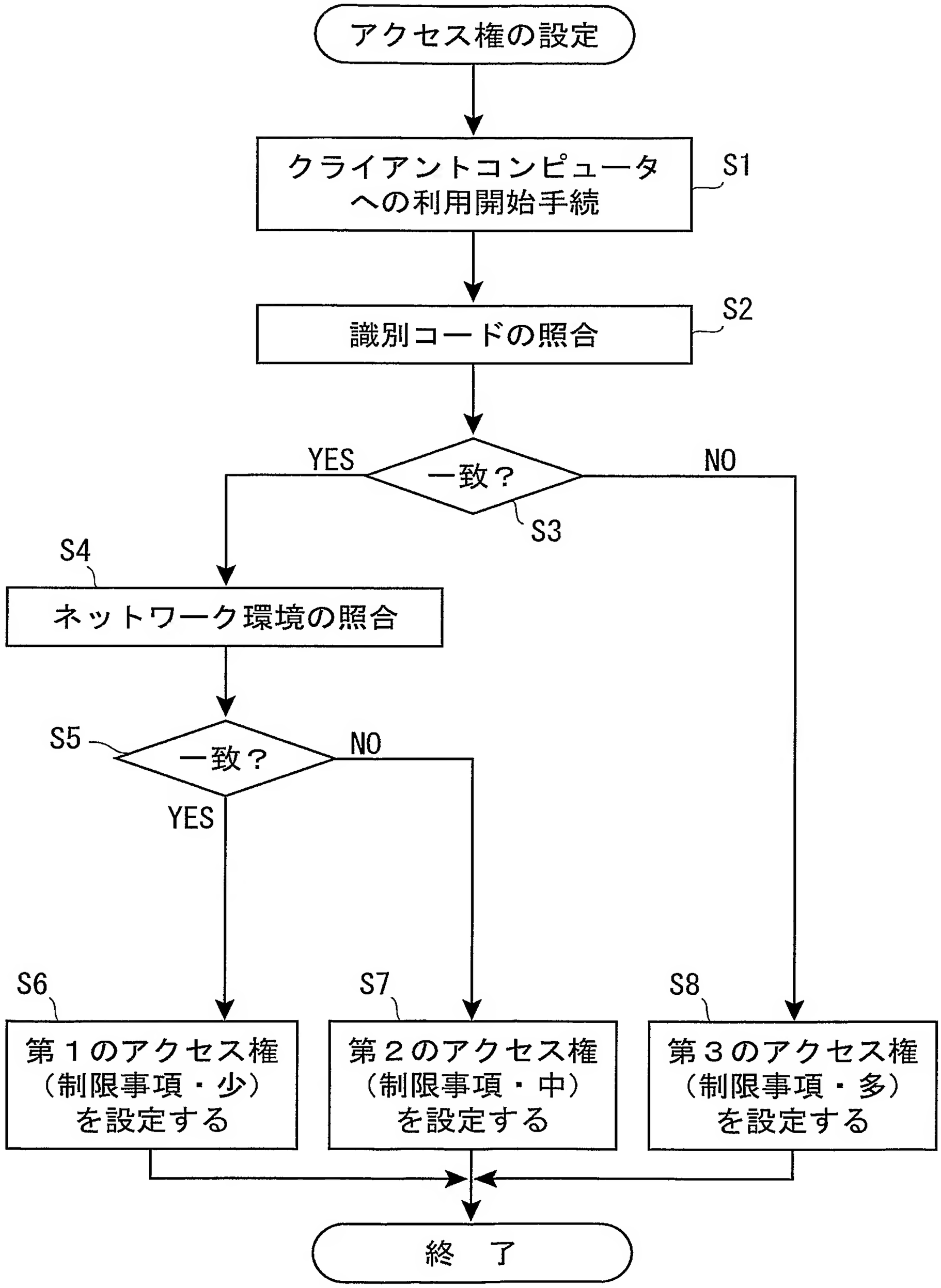
【図１０】


←ネットワーク網へ
ENV(11)
11：クライアント
コンピュータ
11A
サーバアクセス手段
11D
インターフェイス手段
ID(11)
P11：携帯可能
情報処理装置
ID(11)
ENV(11)
11E
11I
識別コード
照合手段
環境
照合手段
11F
アクセス権設定手段
11G
アクセス権伝達手段

【図１１】


アクセス権の設定
クライアントコンピュータへの利用開始手続
S1
識別コードの照合
S2
一致？
S3
YES
NO
ネットワーク環境の照合
S4
S5
一致？
NO
YES
S6
第１のアクセス権（制限事項・少）を設定する
S7
第２のアクセス権（制限事項・中）を設定する
S8
第３のアクセス権（制限事項・多）を設定する
終　了

【図１２】


アクセス権の設定
クライアントコンピュータへの利用開始手続
S1
識別コードの照合
S2
一致？
YES
NO
S3
S4
ネットワーク環境の照合
S5
一致？
NO
YES
S6
第１のアクセス権（制限事項・少）を設定する
S7
第２のアクセス権（制限事項・中）を設定する
S8
第３のアクセス権（制限事項・多）を設定する
終　了

【書類名】要約書
【要約】
【課題】　利用するコンピュータやネットワーク環境に応じて異なるアクセス権を設定する。
【解決手段】　各ユーザ甲，乙，丙に、ＩＣカードＲ１１，Ｒ１２，Ｒ２１を発行する。ユーザ甲のＩＣカードＲ１１内には、ユーザ甲に支給したコンピュータ１１の識別コードＩＤ（１１）と、コンピュータ１１の通常のネットワーク環境を示す環境情報ＥＮＶ（１１）とを記録しておく。各ユーザが、コンピュータを利用するために、ＩＣカードを接続すると、利用対象となるコンピュータの識別コードおよびネットワーク環境が、ＩＣカード内に記録された識別コードおよび環境情報と比較照合され、その一致の程度に応じて、異なるアクセス権が付与される。識別コードとしては、コンピュータに内蔵されたＬＡＮ回路のＭＡＣアドレス、環境情報としては、デフォルトゲートウエイアドレスなどが利用できる。
【選択図】　図８

認定・付加情報

特許出願の番号	特願２００４－０４５９７４
受付番号	５０４００２８４２９３
書類名	特許願
担当官	第七担当上席　００９６
作成日	平成１６年　２月２４日

＜認定情報・付加情報＞

【提出日】　平成16年 2月23日

出証特２００５－３０１５１３６

特願２００４－０４５９７４

出　願　人　履　歴　情　報

識別番号　［０００００２８９７］

１．変更年月日　１９９０年　８月２７日
［変更理由］　新規登録
住　所　東京都新宿区市谷加賀町一丁目１番１号
氏　名　大日本印刷株式会社